Jandeara Kidrycki

Assunto: 1º Diligência - Processo 0000862/2024
Anexos: Relatório de Diligência_BM.pdf

De: experienciawhats <experienciawhats@banrisul.com.br>
Enviada em: quarta-feira, 26 de novembro de 2025 17:00
Para: fernando.dionizio@botmaker.io
Cc: BANRISUL LICITACOES <BANRISUL_LICITACOES@banrisul.com.br>
Assunto: 1º Diligência - Processo 0000862/2024

À BM BRASIL INTERNET LTDA. - 30.607.960/0001-85.

REF.: Licitação Nº 0000862/2024
OBJETO: Prestação de serviços de subscrição de software como serviço (SaaS – Software as a Service) que permita o atendimento por agentes virtuais ou humanos, por meio do aplicativo de mensagens instantâneas Whatsapp, do Grupo Meta.

Prezados,

Solicitamos em diligência os documentos e informações relacionados no arquivo anexo.

O prazo para atendimento é 17.30h do dia 28/11/2025.

Atenciosamente,

Fernanda Jaqueline Reichert
Assistente
Gerência de Estratégia e Soluções Comerciais
Unidade Comercial de Varejo
(51) 3215 2746 | E-mail: Fernanda_reichert@banrisul.com.br

ANTES DE IMPRIMIR este documento pense em sua responsabilidade e compromisso com o MEIO AMBIENTE.

Clique aqui para avaliar meu atendimento

botmaker
UNLEASH HUMAN POTENTIAL

AUTODECLARAÇÃO DE ATENDIMENTO A REQUISITO DE EDITAL E SEUS ANEXOS

BM BRASIL INTERNET LTDA, CNPJ número 30.607.960/0001-85, sediada na Rua Surubim, nº 577 - Conjuntos comerciais no 171 e 172 - 17º Andar, declara para todos os fins legais, que, cumpre plenamente os requisitos listados na tabela abaixo exigidos no EDITAL e seus ANEXOS, estando ciente de todos os seus termos.

Anexo	Item do Edital	Descrição
Especificações do Produto	1.1	Implantar solução in cloud e API WhatsApp.
Especificações do Produto	1.2	Ativação de números na conta WhatsApp Business API.
Especificações do Produto	1.4	Implantar ambientes apartados de produção e laboratório.
Especificações do Produto	1.5	Permitir redundância e contingência dos serviços.
Especificações do Produto	1.6	Atendimento integrado a canais (WhatsApp, SMS, Email, etc).
Especificações do Produto	1.11	Integração ao ambiente legado.
Especificações do Produto	1.12	Integração aos aplicativos do Grupo Banrisul.
Especificações do Produto	1.13	Integração e transbordo com assistente virtual.
Especificações do Produto	1.14	Integração com Consumidor.gov, Reclame Aqui, lojas de apps,analytics.
Especificações do Produto	1.15	Integração com sistemas corporativos via API REST.
Especificações do Produto	1.16	Compatibilidade com CRMs e ferramentas de mercado.
Especificações do Produto	1.18	Integração e ativação de novos números WABA.
Especificações do Produto	1.20	Consultoria de melhoria contínua técnica e de negócio.
Segurança	1.27	Armazenamento em países autorizados pelo BACEN.
Segurança	1.28	Informar mudanças de território ou fornecedor.
Segurança	1.29	Comunicação prévia de mudanças e impactos.
Segurança	1.30	Contratante pode vetar alterações.
LGPD	1.31	Conformidade com a LGPD.
Compatibilidade	2.1	Compatibilidade com Windows suportado.
Compatibilidade	2.2	Compatibilidade com navegadores Edge/Chrome.

Clicksign 0128fcbc-9b20-4fd9-a791-841aeade0b53

Compatibilidade	2.3	Compatibilidade com dispositivos iOS e Android.
Segurança	3.1	Cumprimento das normas de segurança do Contratante.
Segurança	3.2	Subcontratação limitada e informada.
Segurança	3.3	Integrações devem seguir parâmetros de segurança.
Segurança	3.4	Disponibilizar documentação de infraestrutura/arquitetura.
Funcional	4.9	Permitir automatização de monitorias com Speech/Text Analytics.
Banco de Dados	1.1.6	Manutenção/licenciamento de BD quando aplicável.

São Paulo, SP
24/11/2025

Felipe David Cohen
LICITANTE

Telefone: 11 97215-5971
E-mail:felipe.cohen@botmaker.io

Clicksign 0128fcbc-9b20-4fd9-a791-841aeade0b53

19 - AUTODECLARAÇÃO DE ATENDIMENTO A REQUISITO DE EDITAL E SEUS ANEXOS.pdf

Documento número #0128fcbc-9b20-4fd9-a791-841aeade0b53

Hash do documento original (SHA256): eac374a6592aa5c7a1d6db4c0239469e90ed11f4b70aa5d6f8e751a236636226

Assinaturas

Felipe Cohen
Assinou como representante legal em 24 nov 2025 às 09:01:25

Log

24 nov 2025, 07:43:40	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 criou este documento número 0128fcbc-9b20-4fd9-a791-841aeade0b53. Data limite para assinatura do documento: 24 de dezembro de 2025 (07:42). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
24 nov 2025, 07:47:09	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Data limite para assinatura do documento: 24 de novembro de 2025 (16:00).
24 nov 2025, 07:47:09	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Finalização automática após a última assinatura: não habilitada.
24 nov 2025, 07:47:12	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 adicionou à Lista de Assinatura: felipe.cohen@botmaker.io para assinar como representante legal, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Felipe Cohen.
24 nov 2025, 09:01:25	Felipe Cohen assinou como representante legal. Pontos de autenticação: Token via E-mail felipe.cohen@botmaker.io. IP: 177.26.232.98. Localização compartilhada pelo dispositivo eletrônico: latitude -23.57810579346322 e longitude -46.6923699186964. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1346.2 disponibilizado em https://app.clicksign.com.
24 nov 2025, 09:17:05	Operador com email stephanie@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 finalizou o processo de assinatura. Processo de assinatura concluído para o documento número 0128fcbc-9b20-4fd9-a791-841aeade0b53.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 0128fcbc-9b20-4fd9-a791-841aeade0b53, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

DECLARAÇÃO DE COMPATIBILIDADE COM SOLUÇÕES SPEECH ANALYTICS

BM Brasil Internet Ltda, CNPJ nº **30.607.960/0001-85**, sediada à **Rua Surubim, 577, Conjuntos 171 e 172, 17º andar – Cidade Monções – São Paulo/SP – CEP 04571-050**, declara que a **SOLUÇÃO DE ATENDIMENTO B2C** ofertada, compatível com o objeto do presente EDITAL, **é plenamente compatível com soluções de Speech Analytics disponíveis no mercado**, não possuindo qualquer restrição técnica para integração com ferramentas de análise de áudio, transcrição, mineração de voz ou processamento de linguagem natural.

Descrição detalhada das soluções Speech Analytics compatíveis com a SOLUÇÃO cotada pela LICITANTE

Google Speech Analytics & AI Services

Nome da Solução: Google Cloud Speech-to-Text e Natural Language AI
Empresa fornecedora: Google LLC
Modelo de implantação: On Cloud (Google Cloud Platform – GCP)

OpenAI Realtime & Whisper Analytics

Nome da Solução: OpenAI Whisper / Realtime Speech Analysis
Empresa fornecedora: OpenAI, L.L.C.
Modelo de implantação: On Cloud

A solução da Botmaker permite integração via API REST, Webhooks, processamento assíncrono e camadas especializadas de troca de dados, garantindo compatibilidade com outras ferramentas de mercado caso seja requerido futuramente pelo CONTRATANTE.

Ficamos à disposição para mais informações.

São Paulo, SP
24/11/2025

Felipe David Cohen
LICITANTE

Telefone: 11 97215-5971
E-mail:felipe.cohen@botmaker.io

Clicksign 50c5e15f-4312-4320-86f7-0aa231499bee

14 - DECLARAÇÃO DE COMPATIBILIDADE COM SOLUÇÕES SPEECH ANALYTICS.pdf

Documento número #50c5e15f-4312-4320-86f7-0aa231499bee

Hash do documento original (SHA256): 6375fdd3e78d22cad42940fd70e12d5cdc24654bc6a70fba2bdeb20e76bd2809

Assinaturas

Felipe Cohen
Assinou como representante legal em 24 nov 2025 às 09:01:25

Log

24 nov 2025, 07:43:40	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 criou este documento número 50c5e15f-4312-4320-86f7-0aa231499bee. Data limite para assinatura do documento: 24 de dezembro de 2025 (07:42). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
24 nov 2025, 07:47:10	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Data limite para assinatura do documento: 24 de novembro de 2025 (16:00).
24 nov 2025, 07:47:10	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Finalização automática após a última assinatura: não habilitada.
24 nov 2025, 07:47:12	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 adicionou à Lista de Assinatura: felipe.cohen@botmaker.io para assinar como representante legal, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Felipe Cohen.
24 nov 2025, 09:01:25	Felipe Cohen assinou como representante legal. Pontos de autenticação: Token via E-mail felipe.cohen@botmaker.io. IP: 177.26.232.98. Localização compartilhada pelo dispositivo eletrônico: latitude -23.57810579346322 e longitude -46.6923699186964. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1346.2 disponibilizado em https://app.clicksign.com.
24 nov 2025, 09:17:31	Operador com email stephanie@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 finalizou o processo de assinatura. Processo de assinatura concluído para o documento número 50c5e15f-4312-4320-86f7-0aa231499bee.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 50c5e15f-4312-4320-86f7-0aa231499bee, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

DECLARAÇÃO DE COMPATIBILIDADE COM SOLUÇÕES TEXT-TO-SPEECH, SPEECH-TO-TEXT E SPEECH-TO-SPEECH

BM Brasil Internet Ltda, CNPJ nº 30.607.960/0001-85, sediada na Rua Surubim, 577, Conjuntos 171 e 172, 17º andar – Cidade Monções – São Paulo/SP – CEP 04571-050, declara que a SOLUÇÃO DE ATENDIMENTO, compatível com o objeto do presente EDITAL, é plenamente compatível com soluções de Text-To-Speech (TTS), Speech-To-Text (STT) e Speech-To-Speech (STS) amplamente disponíveis no mercado, não possuindo qualquer restrição técnica quanto à integração com mecanismos de síntese de voz, reconhecimento de voz ou transformação direta fala-para-fala.

Descrição detalhada das soluções Text-To-Speech e Speech-To-Text compatíveis com a SOLUÇÃO cotada pela LICITANTE

Speech-to-Text (STT)

Nome da Solução: Soniox Speech Recognition
Empresa fornecedora: Soniox Inc.
Modelo de implantação: On Cloud

Nome da Solução: Google Cloud Speech-to-Text
Empresa fornecedora: Google LLC
Modelo de implantação: On Cloud (Google Cloud Platform – GCP)

Text-to-Speech (TTS)

Nome da Solução: Azure Text-to-Speech
Empresa fornecedora: Microsoft Corporation
Modelo de implantação: On Cloud (Microsoft Azure)

Nome da Solução: Google Cloud Text-to-Speech
Empresa fornecedora: Google LLC
Modelo de implantação: On Cloud (Google Cloud Platform – GCP)

Speech-to-Speech (STS)

Nome da Solução: OpenAI Realtime Speech-to-Speech
Empresa fornecedora: OpenAI, L.L.C.
Modelo de implantação: On Cloud

A solução Botmaker suporta integração via APIs REST, Webhooks e fluxos assíncronos, permitindo uso nativo das soluções da Google, bem como compatibilidade com outras plataformas TTS/STT disponíveis no mercado, caso solicitado pelo CONTRATANTE.

Ficamos à disposição para mais informações.

São Paulo, SP
24/11/2025

Felipe David Cohen
LICITANTE
(Assinaturas Digitais)
Telefone: 11 97215-5971
E-mail:felipe.cohen@botmaker.io

Clicksign 8381fbd2-b40a-4f49-ad31-d8903bafee08

13 - DECLARAÇÃO DE COMPATIBILIDADE COM SOLUÇÕES TEXT-TO-SPEECH E SPEECH-TO-TEXT.pdf

Documento número #8381fbd2-b40a-4f49-ad31-d8903bafee08

Hash do documento original (SHA256): c1b2b38d136f76ab18ca15a7eb9eec91ae03748ee90b9bbd1b530dee198b3e54

Assinaturas

Felipe Cohen
Assinou como representante legal em 24 nov 2025 às 09:01:25

Log

24 nov 2025, 07:43:40	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 criou este documento número 8381fbd2-b40a-4f49-ad31-d8903bafee08. Data limite para assinatura do documento: 24 de dezembro de 2025 (07:42). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
24 nov 2025, 07:47:10	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Data limite para assinatura do documento: 24 de novembro de 2025 (16:00).
24 nov 2025, 07:47:10	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Finalização automática após a última assinatura: não habilitada.
24 nov 2025, 07:47:12	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 adicionou à Lista de Assinatura: felipe.cohen@botmaker.io para assinar como representante legal, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Felipe Cohen.
24 nov 2025, 09:01:25	Felipe Cohen assinou como representante legal. Pontos de autenticação: Token via E-mail felipe.cohen@botmaker.io. IP: 177.26.232.98. Localização compartilhada pelo dispositivo eletrônico: latitude -23.57810579346322 e longitude -46.6923699186964. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1346.2 disponibilizado em https://app.clicksign.com.
24 nov 2025, 09:17:17	Operador com email stephanie@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 finalizou o processo de assinatura. Processo de assinatura concluído para o documento número 8381fbd2-b40a-4f49-ad31-d8903bafee08.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 8381fbd2-b40a-4f49-ad31-d8903bafee08, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

botmaker
UNLEASH HUMAN POTENTIAL

DECLARAÇÃO DE NÃO UTILIZAÇÃO DE COMPONENTES DE SOFTWARE OPEN SOURCE

A BM Brasil Internet Ltda, com sede na Rua Surubim, 577, Conjuntos 171 e 172, 17º andar – Cidade Monções – São Paulo/SP – CEP 04571-050, inscrita no CNPJ sob o nº 30.607.960/0001-85, por meio de seu representante legal infra-assinado, FELIPE DAVID COHEN, portador(a) da Cédula de Identidade nº 106421803 e CPF nº 079.240.597-84, DECLARA para os devidos fins de participação na Licitação 13.303/16 Eletrônica, promovida pelo BANCO DO ESTADO DO RIO GRANDE DO SUL S.A.- BANRISUL, regida pelo Edital 0000862/2024:

Que NÃO UTILIZA componentes de software Open Source (código aberto) em suas soluções, objeto da presente licitação.

Por ser expressão da verdade, firmamos a presente declaração.

São Paulo, 24 de Novembro de 2025.

_____

BM Brasil Internet Ltda

CNPJ: 30.607.960/0001-85

Felipe David Cohen

Diretor Financeiro

Clicksign 623e325f-eb4f-4667-8b58-300a5e2a408c

20 - DECLARAÇÃO DE NÃO UTILIZAÇÃO DE COMPONENTES DE SOFTWARE OPEN SOURCE.pdf

Documento número #623e325f-eb4f-4667-8b58-300a5e2a408c

Hash do documento original (SHA256): 0011c8a8f1b065568e0148bacea5ee199fb544ff58dfc57d223e9ef863326b22

Assinaturas

Felipe Cohen
Assinou como representante legal em 24 nov 2025 às 09:01:25

Log

24 nov 2025, 07:43:40	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 criou este documento número 623e325f-eb4f-4667-8b58-300a5e2a408c. Data limite para assinatura do documento: 24 de dezembro de 2025 (07:42). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
24 nov 2025, 07:47:11	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Data limite para assinatura do documento: 24 de novembro de 2025 (16:00).
24 nov 2025, 07:47:11	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Finalização automática após a última assinatura: não habilitada.
24 nov 2025, 07:47:12	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 adicionou à Lista de Assinatura: felipe.cohen@botmaker.io para assinar como representante legal, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Felipe Cohen.
24 nov 2025, 09:01:25	Felipe Cohen assinou como representante legal. Pontos de autenticação: Token via E-mail felipe.cohen@botmaker.io. IP: 177.26.232.98. Localização compartilhada pelo dispositivo eletrônico: latitude -23.57810579346322 e longitude -46.6923699186964. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1346.2 disponibilizado em https://app.clicksign.com.
24 nov 2025, 09:16:32	Operador com email stephanie@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 finalizou o processo de assinatura. Processo de assinatura concluído para o documento número 623e325f-eb4f-4667-8b58-300a5e2a408c.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 623e325f-eb4f-4667-8b58-300a5e2a408c, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

botmaker
UNLEASH HUMAN POTENTIAL

DECLARAÇÃO DE QUALIFICAÇÃO PESSOAL

BM BRASIL INTERNET LTDA, CNPJ nº 30.607.960/0001-85, sediada na Rua Surubim, nº 577, Conjuntos 171 e 172, 17º andar – Brooklin Novo, São Paulo/SP – CEP 04571-050, declara para todos os fins legais que SILVIO GERALDO BOTELHO VAZ, CPF nº 274.124.848-69, está qualificado a prestar serviços de arquitetura, implantação, operação e evolução de soluções de atendimento digital e automação omnichannel, incluindo integrações com APIs, CRMs, sistemas legados, mensageria corporativa, agentes de IA e fluxos conversacionais inteligentes, para a SOLUÇÃO DE ATENDIMENTO, compatível com o objeto do presente EDITAL.

Relação de Certificações do colaborador

CertiProf
- Scrum Foundation Professional Certification – SFPC™
- DevOps Essentials Professional Certificate – DEPC®

AWS – Ka Solution
- AWS Cloud Practitioner Essentials
- Securing Your AWS Cloud
- Strategies and Tools for Large-Scale Migrations
- Fundamentals of a Modern Data Strategy on AWS and Machine Learning Basics

Microsoft – Ka Solution
- Microsoft 365 Fundamentals (MS-900)
- Power Platform Fundamentals (PL-900)

Governança e Segurança
- Cobit
- Cobit 4.0
- DPO & LGPD
- ITIL Foundation

Qualidade e Processos
- Six Sigma – Yellow Belt

Formação Acadêmica

UNIP – Universidade Paulista
- Bacharelado em Administração – Conclusão: 2000
- Bacharelado em Economia – Conclusão: 2009

Clicksign 7b80f556-25b1-448e-ab0d-6f57a8d04f46

botmaker
UNLEASH HUMAN POTENTIAL

Experiência Profissional

Head of Conversational AI & Chatbot Development – Botmaker
Fev/2025 – Atual

• Lidera squads multifuncionais compostas por PMs, chatbot developers, software engineers e data analysts, responsáveis pelo design, refatoração e entrega de soluções conversacionais avançadas.
• Gerencia projetos de IA conversacional end-to-end nos setores de educação, serviços financeiros, automotivo, varejo e telecom, desde discovery e levantamento de requisitos até go-live e governança evolutiva.
• Arquiteta fluxos conversacionais com Meta Flows, generative AI e Connection Actions (CA), integrando com CRMs (Salesforce, HubSpot, Pipedrive), ERPs e APIs corporativas.
• Implementa modelos de governança técnica e operacional para squads de Delivery, com KPIs de lead time, throughput, eficiência, estabilidade e qualidade.
• Principais entregas: bots de geração de leads para universidades, agentes de renegociação para instituições financeiras, fluxos de agendamento e test-drive para montadoras, automações omnichannel em segmentos de grande escala.

Principais Competências Técnicas e Funcionais

• Arquitetura de soluções de IA conversacional, Meta Flows, CAs e integrações com mensageria corporativa.
• Desenvolvimento e evolução de chatbots, voicebots, automações e agentes autônomos.
• Integrações com CRMs (Salesforce, HubSpot, Pipedrive), ERPs e plataformas proprietárias via APIs REST.
• Governança de projetos (Scrum/Kanban), gestão de squads multidisciplinares e práticas de agilidade escalada.
• Conhecimentos sólidos em ambientes cloud (AWS, Azure), modelos de dados, segurança e conformidade.
• Monitoria, métricas, KPIs e analytics aplicados a atendimento digital e operações de IA.
• Experiência em negociação técnica e definição de roadmap com stakeholders executivos.

Relação dos softwares integrantes da SOLUÇÃO de expertise do colaborador

• Botmaker Platform (construção e operação de chatbots, voicebots e automações)
• Meta WhatsApp Business API / Meta Flows / Connection Actions (CA)
• APIs REST, Webhooks e integrações corporativas (CRM, ERP, Middleware, Gateways)
• Plataformas de CRM: Salesforce, HubSpot, Pipedrive
• Ambientes Cloud (AWS, GCP, Azure)
• Ferramentas de governança ágil (Scrum/Kanban) e monitoria operacional
• Ferramentas de analytics e métricas aplicadas ao atendimento digital

São Paulo, SP
24/11/2025

Felipe David Cohen
LICITANTE
Telefone: 11 97215-5971
E-mail:felipe.cohen@botmaker.io

Clicksign 7b80f556-25b1-448e-ab0d-6f57a8d04f46

15 - Banrisul - DECLARAÇÃO DE QUALIFICAÇÃO PESSOAL.pdf

Documento número #7b80f556-25b1-448e-ab0d-6f57a8d04f46

Hash do documento original (SHA256): c88c220876deec7b19d795189646c7c99d57ecf0a1f292749dfc73efc51c1fae

Assinaturas

Felipe Cohen
Assinou como representante legal em 24 nov 2025 às 09:01:24

Log

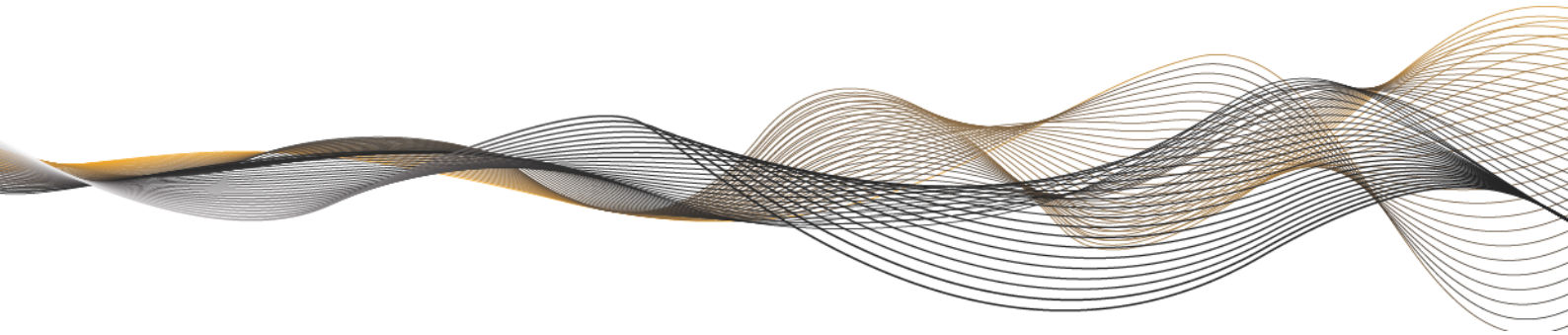
24 nov 2025, 07:43:40	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 criou este documento número 7b80f556-25b1-448e-ab0d-6f57a8d04f46. Data limite para assinatura do documento: 24 de dezembro de 2025 (07:42). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
24 nov 2025, 07:47:09	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Data limite para assinatura do documento: 24 de novembro de 2025 (16:00).
24 nov 2025, 07:47:09	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Finalização automática após a última assinatura: não habilitada.
24 nov 2025, 07:47:12	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 adicionou à Lista de Assinatura: felipe.cohen@botmaker.io para assinar como representante legal, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Felipe Cohen.
24 nov 2025, 09:01:24	Felipe Cohen assinou como representante legal. Pontos de autenticação: Token via E-mail felipe.cohen@botmaker.io. IP: 177.26.232.98. Localização compartilhada pelo dispositivo eletrônico: latitude -23.57810579346322 e longitude -46.6923699186964. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1346.2 disponibilizado em https://app.clicksign.com.
24 nov 2025, 09:17:11	Operador com email stephanie@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 finalizou o processo de assinatura. Processo de assinatura concluído para o documento número 7b80f556-25b1-448e-ab0d-6f57a8d04f46.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 7b80f556-25b1-448e-ab0d-6f57a8d04f46, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

BASE4 SECURITY

ARG - MEX - CL - BRA - COL - PE - ESP - EEUU



Pentest Web

Informe Técnico de Re-Test

BotMaker

Viernes, 24 de Enero de 2025

Confidencialidad del documento

Toda información contenida en el presente documento deberá mantenerse en forma estrictamente confidencial. Prohibido copiar y reproducir este documento o parte de este sin la debida autorización de BASE4 Security. Las obligaciones señaladas continuarán vigentes aún después de su vencimiento o terminación de uso de la presente propuesta.

Este documento se ha preparado para uso interno del Cliente, por lo tanto, se espera que el lector de este sea empleado autorizado de esta organización. Las metodologías, procedimientos y procesos utilizados, se realizan como parte de los servicios profesionales que BASE4 Security ofrece, estos son parte de su conocimiento de consultoría y asesoría y por lo tanto hacen parte de activos intangibles y propiedad intelectual. Se solicita amablemente el uso ético y profesional de esta información. El Cliente se obliga a que toda la información contenida en este documento no sea de acceso público. Esta información deberá ser mantenida en forma estrictamente confidencial y utilizada exclusivamente para el desarrollo de la presente actividad. Igualmente, El Cliente se compromete a tomar todas las medidas necesarias para que la información contenida en este documento no llegue a manos de terceros en ninguna circunstancia y se obliga a no utilizarla para ningún objeto diferente al de adelantar las tareas derivadas de la presente actividad.

Índice de contenidos

Confidencialidad del documento 2

Resumen Ejecutivo 4

- Objetivo 4
- Alcance 4
- Cuentas de Usuario 4
- Duración del Proyecto 4
- Clasificación de Riesgo 6
- Resultados 8

Vulnerabilidades 10

- Resumen de vulnerabilidades 10

Conclusión 36

Proceso de Pentest Web 38

- OWASP Web Security Testing Guide 38
- OWASP Top 10 - 2021 41

Apéndices 44

Resumen Ejecutivo

Objetivo

Presentar el **Informe Técnico de Re-Test** con los resultados del proyecto de **Pentest Web** de tipo **GreyBox** realizado a los activos indicados por **BotMaker**. Este tipo de análisis tiene como objetivo fundamental la detección oportuna de las vulnerabilidades de seguridad que pudieran presentar los sistemas de la compañía, teniendo en cuenta que, de no ser reconocidos y solucionados, potenciales atacantes podrían intentar comprometer la confidencialidad, integridad y disponibilidad de la información contenida en éstos.

Alcance

El proyecto de **Pentest Web** comprendió la evaluación de seguridad de los siguientes activos:

Prueba	Aplicación	URL
Grey Box	BotMaker	https://go.botmaker.com

Cuentas de Usuario

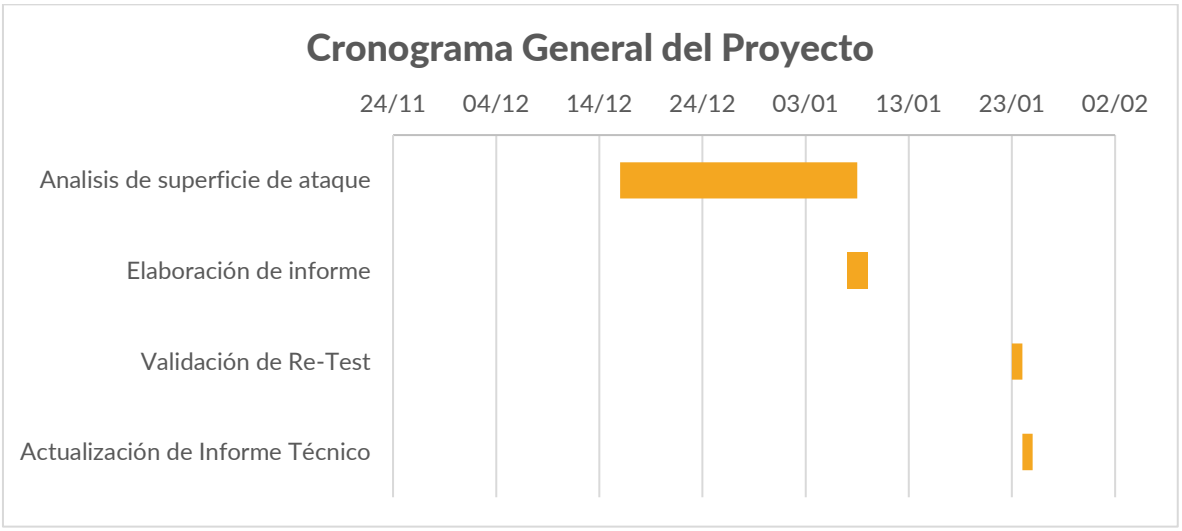
Para la ejecución de las tareas del **Pentest Web** fueron provistas las siguientes cuentas de usuario:

Usuario	Descripción
jtommasi@base4sec.com	Usuario con el rol SuperAdministrador

Duración del Proyecto

Las tareas del proyecto de **Pentest Web** fueron realizadas de acuerdo con el siguiente cronograma y tuvieron una duración total de **15 días**.

Actividad	Fecha de Inicio	Fecha Final
Análisis de superficie de ataque	16-12-2024	07-01-2025
Elaboración de informe	07-01-2025	08-01-2025
Validación de Re-Test	23-01-2025	23-01-2025
Actualización de Informe Técnico	24-01-2025	24-01-2025



Clasificación de Riesgo

Durante la ejecución de un proyecto, los consultores de seguridad de Base4 Security trabajan con las siguientes metodologías a fin de poder reflejar con mayor precisión técnica el riesgo final de las vulnerabilidades que se pudieran hallar en los activos analizados:

CVSS v3.1 (Common Vulnerability Scoring System)

CVSS es un sistema de puntaje diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en Tecnologías de la Información (IT), es decir, contribuye a cuantificar la severidad que pueden representar dichas vulnerabilidades. Una vez que los valores de las métricas Base son asignadas por un analista, la ecuación definida para calcular la puntuación genera un valor entre 0.0 y 10.0 derivada de dos subcálculos procedentes de las métricas de Explotación e Impacto.

Riesgo	Puntuación	Definición
CRÍTICO	9.0 – 10.0	• Explotación simple • No se requieren privilegios del sistema ni interacción con usuario • Perdida de confidencialidad, integridad y disponibilidad del sistema afectado • Se recomienda formar un plan de acción y remediar de inmediato
ALTO	7.0 – 8.9	• Complejidad del ataque es baja • Se requieren privilegios del sistema, pero no interacción con usuario • Impacto alto en Confidencialidad, Integridad y Disponibilidad del sistema afectado • Se recomienda formar un plan de acción y remediar lo antes posible
MEDIO	4.0 – 6.9	• Complejidad del ataque es alta • Se requieren privilegios del sistema o interacción con usuario • Impacto en por lo menos una de Confidencialidad, Integridad o Disponibilidad del sistema afectado • Se recomienda formar un plan de acción y remediar después de los problemas de alta prioridad

BAJO	0.1 – 3.9	• Vulnerabilidad muy difícil de explotar • Impacto es mínimo • Se recomienda formar un plan de acción y remediar en la próxima ventana de mantenimiento

OWASP (Open Web Application Security Project)

Acorde a la metodología OWASP, para determinar la severidad del riesgo se debe trabajar con los siguientes valores:

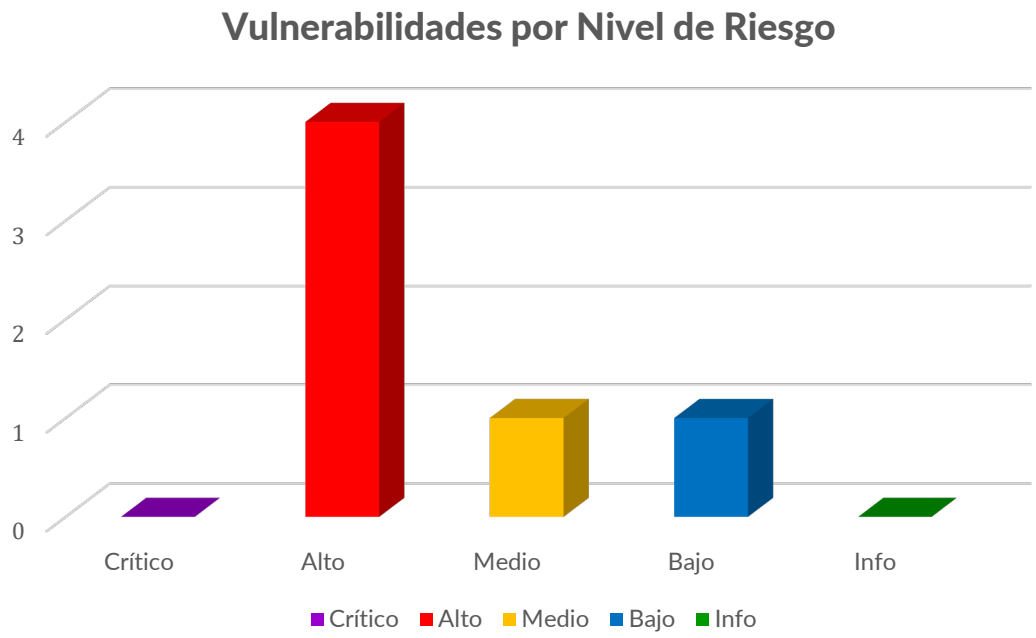
- **Probabilidad de la ocurrencia de la amenaza (PROBABILIDAD)** En este punto se intenta lograr identificar cuál es la amenaza y las vulnerabilidades que puedan ser aprovechadas para comprometer los activos de la empresa y la seguridad de la información que éstos contengan o manejen. Se analiza que tan probable una determinada vulnerabilidad puede ser descubierta y aprovechada con éxito.
- **Impacto generado sobre el negocio (IMPACTO)** Se debe determinar el impacto que la vulnerabilidad tendrá tanto en el aspecto técnico como así también en el negocio de la empresa. En cuanto al Impacto Técnico, se contemplan la pérdida de la confidencialidad, integridad, disponibilidad y auditabilidad de la información. El Impacto en el Negocio se mide según el daño económico, de la imagen de la compañía, la violación de la privacidad de las personas afectadas, como así también la falla en el cumplimiento de regulaciones.

RIESGO = PROBABILIDAD * IMPACTO

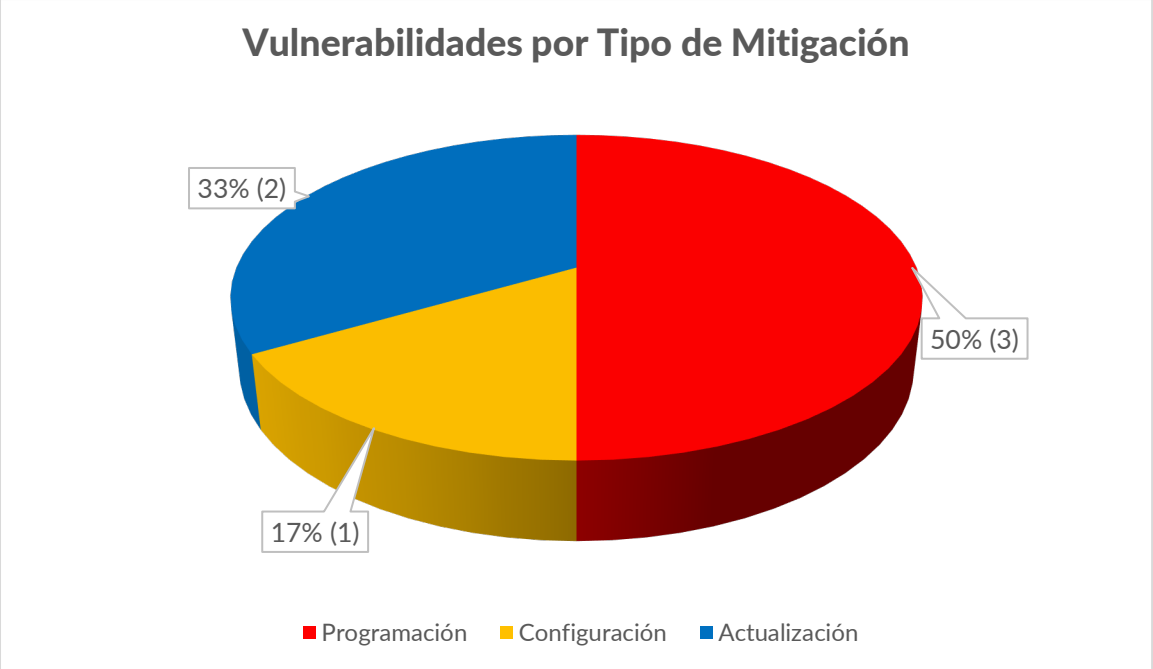


Resultados

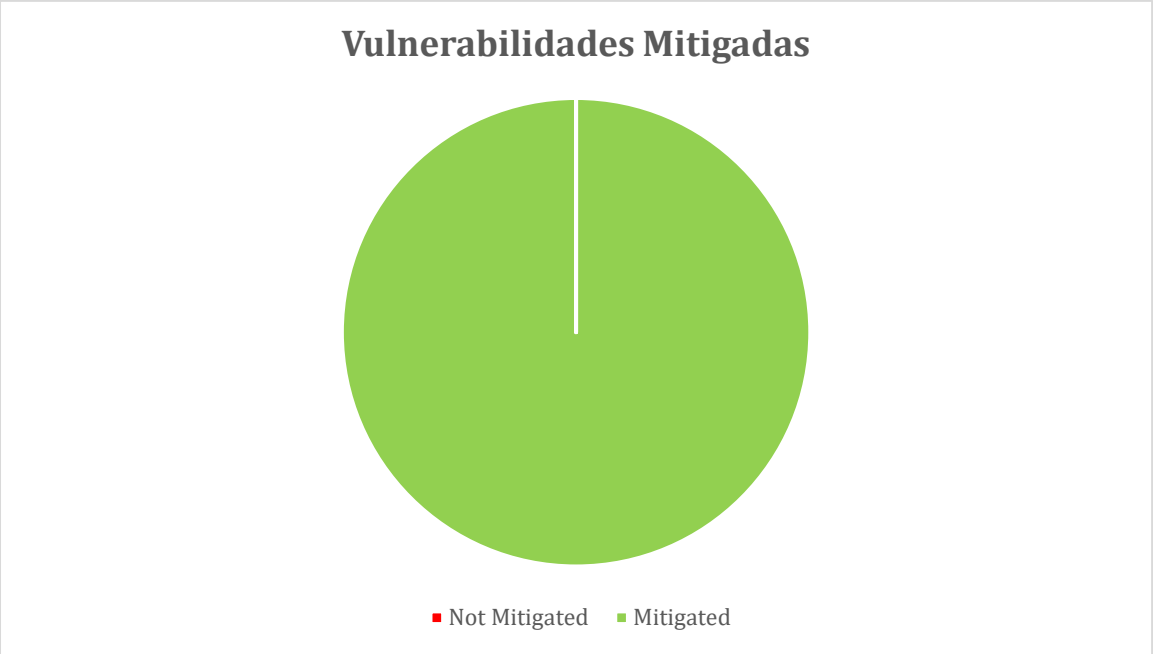
Como resultado de las pruebas de seguridad realizadas sobre los activos especificados en el alcance, se han identificado **cero (0)** vulnerabilidades de riesgo **Crítico**, **cuatro (4)** vulnerabilidades de riesgo **Alto**, **una (1)** vulnerabilidad de riesgo **Medio**, **una (1)** vulnerabilidad de riesgo **Bajo** y **cero (0)** vulnerabilidades de riesgo **Informativo**. Se recomienda revisar las vulnerabilidades halladas y mitigarlas lo antes posible, acorde a las posibilidades y prioridades del negocio.



Asimismo, se determinó que, del total de vulnerabilidades detectadas, **tres (3)** corresponden a errores de **Programación**, **uno (1)** corresponden a errores de **Configuración** y **dos (2)** corresponden a falta de **Actualización**.



Para los resultados de **RETEST** de las vulnerabilidades detectadas se ha identificado que todos los issues han sido mitigados.



Vulnerabilidades

Resumen de vulnerabilidades

A continuación, se presentan las vulnerabilidades encontradas en los activos especificados en el alcance, junto a su riesgo calculado acorde a la metodología OWASP:

ID	Vulnerabilidad	Impacto	Probabilidad	Riesgo	CVSS	Activos Afectados
A1	Uso de software vulnerable Jetty 9.4.48	Alto	Media	Alto	8.1	go.botmaker.com
A2	Uso de software deprecado Jetty 12.0.8	Alto	Media	Alto	8.1	go.botmaker.com
A3	Stored XSS	Alto	Media	Alto	7.3	go.botmaker.com
A4	ServerSide Request Forgery (localhost bypass)	Medio	Alta	Alto	7.7	ws.botmaker.com
M1	Software Information Disclosure	Bajo	Alta	Medio	5.3	go.botmaker.com
B1	Path Traversal: Acciones de Código	Bajo	Medio	Bajo	3.1	go.botmaker.com

A1. Uso de software vulnerable Jetty 9.4.48

Descripción					
Activo(s) Afectado(s)	• https://go.botmaker.com/				
Impacto	Alto	Probabilidad	Media	Riesgo	Alto
CVE/CWE	CWE-1104: Use of Unmaintained Third Party Components		Mitigación	Mitigado	
OWASP	A06:2021 – Vulnerable and Outdated Components		Remediación	**Actualización**	
CVSSv3.1	8.1				
Mitre ATT&CK	N/A				

Vulnerabilidad

Jetty, en su versión **9.4.48.v20220622**, presenta múltiples vulnerabilidades que pueden comprometer la seguridad de las aplicaciones que dependen de este servidor web. Estas vulnerabilidades abarcan desde la denegación de servicio hasta la exposición de información sensible y la aceptación incorrecta de encabezados HTTP. Cada problema surge de diferentes fallos en la implementación del servidor:

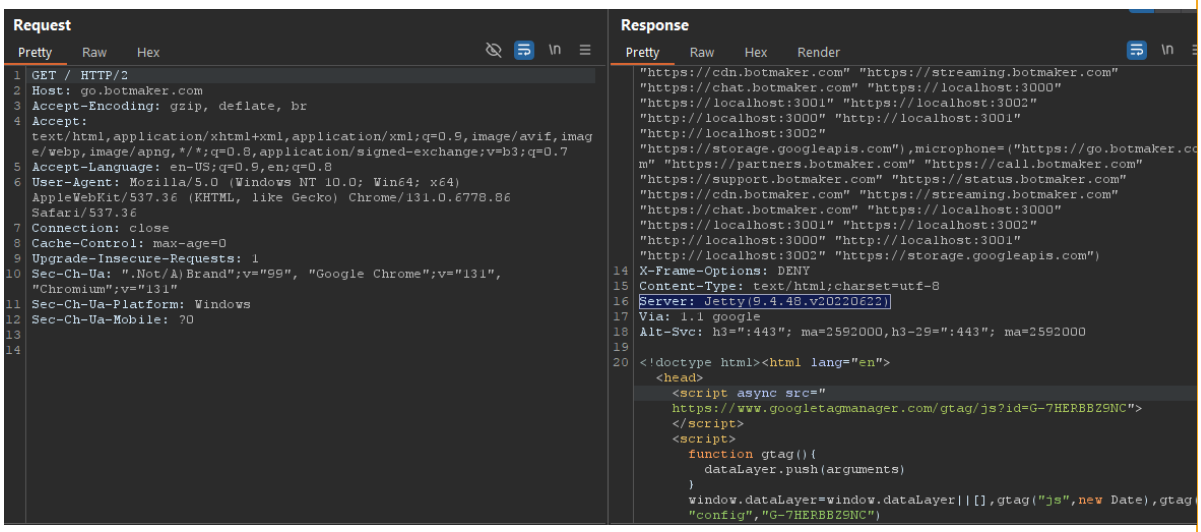
CVE-2023-26048: Un fallo en la gestión de memoria en las funciones HttpServletRequest.getParameter() y HttpServletRequest.getParts() permite a un atacante remoto enviar solicitudes multipartitas maliciosas que agotan los recursos del servidor, resultando en una condición de denegación de servicio (DoS).

CVE-2023-26049: Un defecto en la interpretación de cookies no estándar puede exponer información sensible. Las cookies malformadas son procesadas de manera insegura, lo que podría permitir a atacantes autenticados obtener datos que no deberían ser accesibles.

CVE-2023-40167: Jetty acepta el carácter + en el valor del encabezado Content-Length, lo que contradice el estándar del RFC HTTP/1.1. Este comportamiento podría ser explotado para evadir controles de seguridad, especialmente en entornos donde se confía en la validación estricta de encabezados.

Proceso y Evidencia

A través de la cabecera **Server:** identificada en la vulnerabilidad **B1**, se ha realizado la investigación de la versión, la cual está fuera de soporte (EOL) y que presenta múltiples vulnerabilidades. A continuación se muestra la evidencia de lo descrito anteriormente, donde se puede observar el banner en cuestión:



Impacto

El impacto de estas vulnerabilidades varía según el escenario, pero afecta elementos esenciales de la seguridad operativa:

Disponibilidad: Las condiciones de denegación de servicio, como las descritas en **CVE-2023-26048**, pueden interrumpir operaciones críticas, afectando tanto a usuarios finales como a procesos internos. La inactividad prolongada puede generar pérdidas financieras y dañar la reputación de las organizaciones.

Confidencialidad: El fallo de **CVE-2023-26049** puede resultar en la exposición de información sensible almacenada en cookies. Esta fuga de datos puede ser

aprovechada para realizar ataques más sofisticados, como suplantación de identidad o escalamiento de privilegios.

Integridad: Aunque no directamente alterada por estas vulnerabilidades, la aceptación incorrecta de valores de encabezados HTTP (**CVE-2023-40167**) podría facilitar técnicas avanzadas de manipulación o evasión que afecten la confiabilidad del sistema.

Recomendación

La principal medida de mitigación para las vulnerabilidades identificadas en **Jetty** es actualizar el servidor a la versión más reciente disponible al día de hoy, proporcionada por los mantenedores del proyecto **Eclipse Jetty**. Las actualizaciones incluyen parches de seguridad diseñados para abordar específicamente los problemas detectados. Además de la actualización, se recomienda realizar las siguientes acciones para fortalecer la seguridad del entorno:

Revisión de Configuración: Asegúrese de que la configuración del servidor siga las mejores prácticas, limitando el tamaño de las solicitudes multipartitas y utilizando reglas estrictas para la validación de encabezados HTTP.
Monitoreo Continuo: Implemente herramientas de monitoreo en tiempo real que identifiquen patrones de uso inusual de recursos o actividad sospechosa en el servidor.

Al mantener el servidor actualizado y aplicar medidas de seguridad complementarias, se reduce significativamente el riesgo de explotación de estas vulnerabilidades.

Referencias

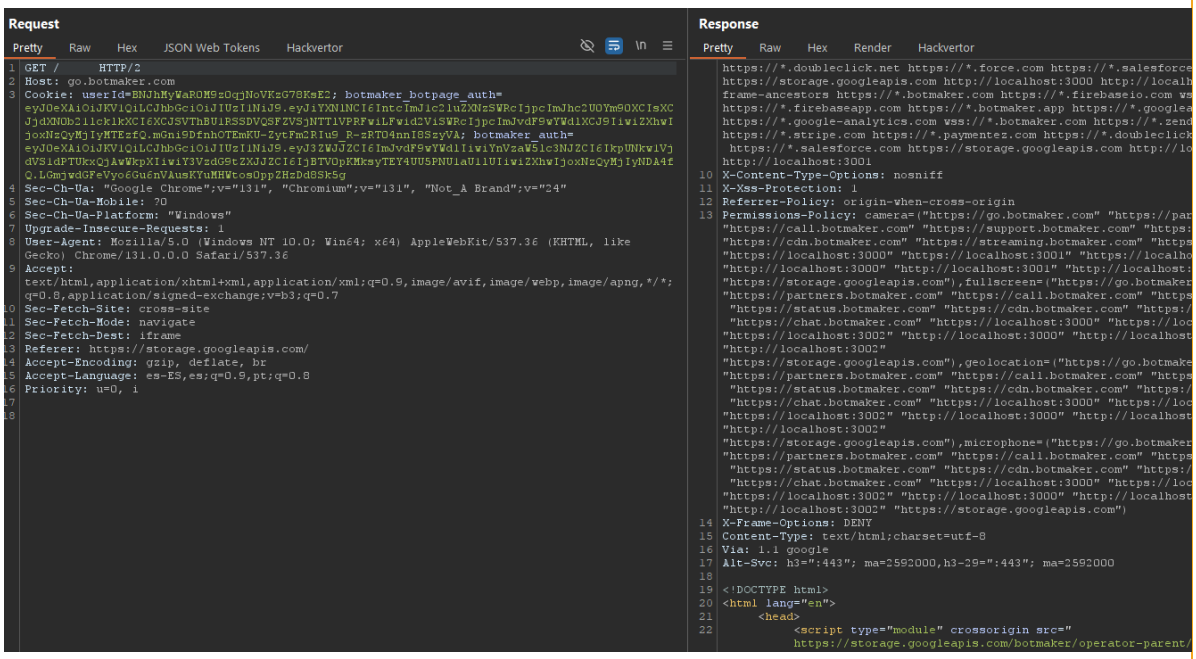
Puede visitar los siguientes enlaces para más información:

- https://nvd.nist.gov/vuln/detail/CVE-2023-26048
- https://nvd.nist.gov/vuln/detail/CVE-2023-26049

- https://nvd.nist.gov/vuln/detail/CVE-2023-40167

Re-Test

Durante la fase inicial de evaluación de seguridad, se detectó que el servidor web utilizaba una versión vulnerable de Jetty (9.4.48), lo cual representaba un riesgo significativo debido a las vulnerabilidades conocidas en dicha versión. En el retest, se verificó que el banner del servidor ya no es visible, lo que impide confirmar si la versión vulnerable ha sido actualizada. Aunque no se ha podido corroborar la actualización a una versión segura, el cambio realizado mitiga el riesgo inicial al ocultar información sensible sobre la tecnología empleada. Por tanto, este hallazgo se considera mitigado. A continuación puede ver la evidencia de lo descrito:



A2. Uso de software deprecado Jetty 12.0.8

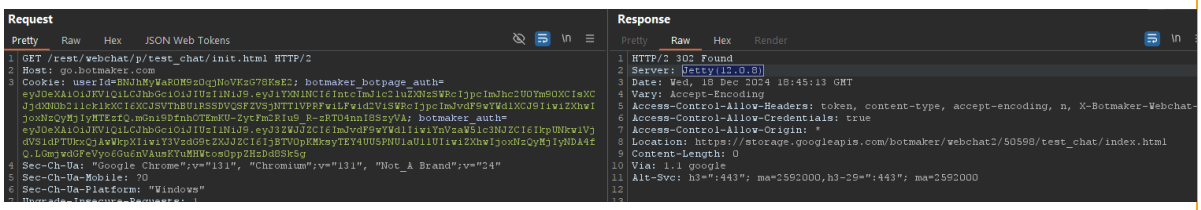
Descripción					
Activo(s) Afectado(s)	• https://go.botmaker.com/				
Impacto	Alto	Probabilidad	Media	Riesgo	Alto
CVE/CWE	CWE-1104: Use of Unmaintained Third Party Components		Mitigación	Mitigado	
OWASP	A06:2021 – Vulnerable and Outdated Components		Remediación	**Actualización**	
CVSSv3.1	8.1				
Mitre ATT&CK	N/A				

Vulnerabilidad

Se ha identificado el uso de la versión **Jetty 12.0.8** en el entorno de producción de la aplicación. Aunque esta versión no presenta vulnerabilidades conocidas, se encuentra en estado **End-of-Life (EOL),** lo que significa que ya no recibe actualizaciones de seguridad, soporte técnico ni parches por parte de sus desarrolladores. Esto representa un riesgo latente para la seguridad y estabilidad del sistema, ya que futuras vulnerabilidades que puedan ser descubiertas en esta versión no serán corregidas, dejando la aplicación expuesta a posibles ataques. El uso de software deprecado también puede implicar incompatibilidades con futuras actualizaciones de sistemas operativos, bibliotecas y otras dependencias críticas, comprometiendo la capacidad del sistema para mantenerse actualizado y seguro en el tiempo.

Proceso y Evidencia

A continuación se muestra la evidencia en la respuesta http del sitio la versión de **Jetty 12.0.8** la cual ya no posee parches de seguridad ni soporte técnico:



Impacto

El impacto del uso de software en estado EOL radica en la exposición a riesgos potenciales debido a la ausencia de soporte y parches de seguridad. Aunque actualmente no se han identificado vulnerabilidades específicas en **Jetty 12.0.8**, el software deprecado aumenta significativamente la superficie de ataque del sistema y puede ser un vector atractivo para atacantes una vez que surjan vulnerabilidades públicas. Esto compromete la confidencialidad de los datos al facilitar posibles brechas de seguridad, pone en riesgo la integridad de la aplicación al permitir la explotación de futuras fallas no corregidas y afecta la disponibilidad al exponer el entorno a posibles interrupciones derivadas de ataques. Asimismo, el uso de software EOL puede impactar en el cumplimiento normativo y en la reputación de la organización, especialmente si se producen incidentes de seguridad que podrían haberse mitigado actualizando a una versión soportada.

Recomendación

Es altamente recomendable migrar la implementación de Jetty a una versión soportada y que reciba actualizaciones de seguridad regulares. Se debe identificar la versión más reciente y estable de Jetty que sea compatible con la aplicación y proceder con un plan de actualización cuidadosamente ejecutado. Este proceso incluye la validación de compatibilidad con dependencias, la realización de pruebas exhaustivas en un entorno de staging y la actualización progresiva en los entornos de desarrollo, prueba y producción. Además, se sugiere documentar el proceso de

migración y establecer un monitoreo continuo para futuras alertas de EOL o vulnerabilidades relacionadas con los componentes utilizados.

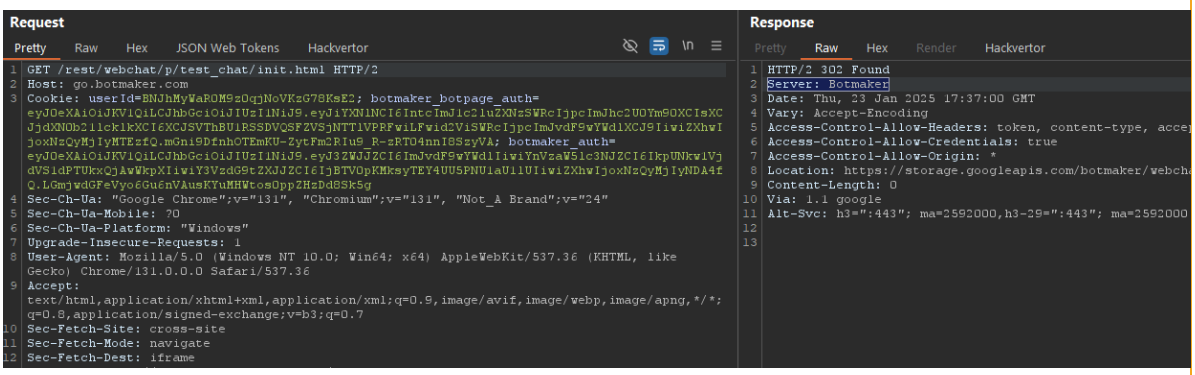
Referencias

Puede visitar los siguientes enlaces para más información:

- https://cwe.mitre.org/data/definitions/1104.html

Re-Test

Durante la fase inicial de evaluación de seguridad, se detectó que el servidor web utilizaba una versión vulnerable de **Jetty (12.0.8),** lo cual representaba un riesgo significativo debido a las vulnerabilidades conocidas en dicha versión. En el retest, se verificó que el banner del servidor ya no es visible, lo que impide confirmar si la versión vulnerable ha sido actualizada. Aunque no se ha podido corroborar la actualización a una versión segura, el cambio realizado mitiga el riesgo inicial al ocultar información sensible sobre la tecnología empleada. Por tanto, este hallazgo se considera mitigado. A continuación puede ver la evidencia de lo descrito:



A3. Stored XSS

Descripción					
Activo(s) Afectado(s)	• https://go.botmaker.com/rest/operator/uploadResource				
Impacto	Alto	Probabilidad	Media	Riesgo	Alto
CVE/CWE	CWE-434: Unrestricted File Upload CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		Mitigación	Mitigado	
OWASP	A05:2021 - Security Misconfiguration		Remediación	**Programación**	
CVSSv3.1	7.3				
Mitre ATT&CK	N/A				

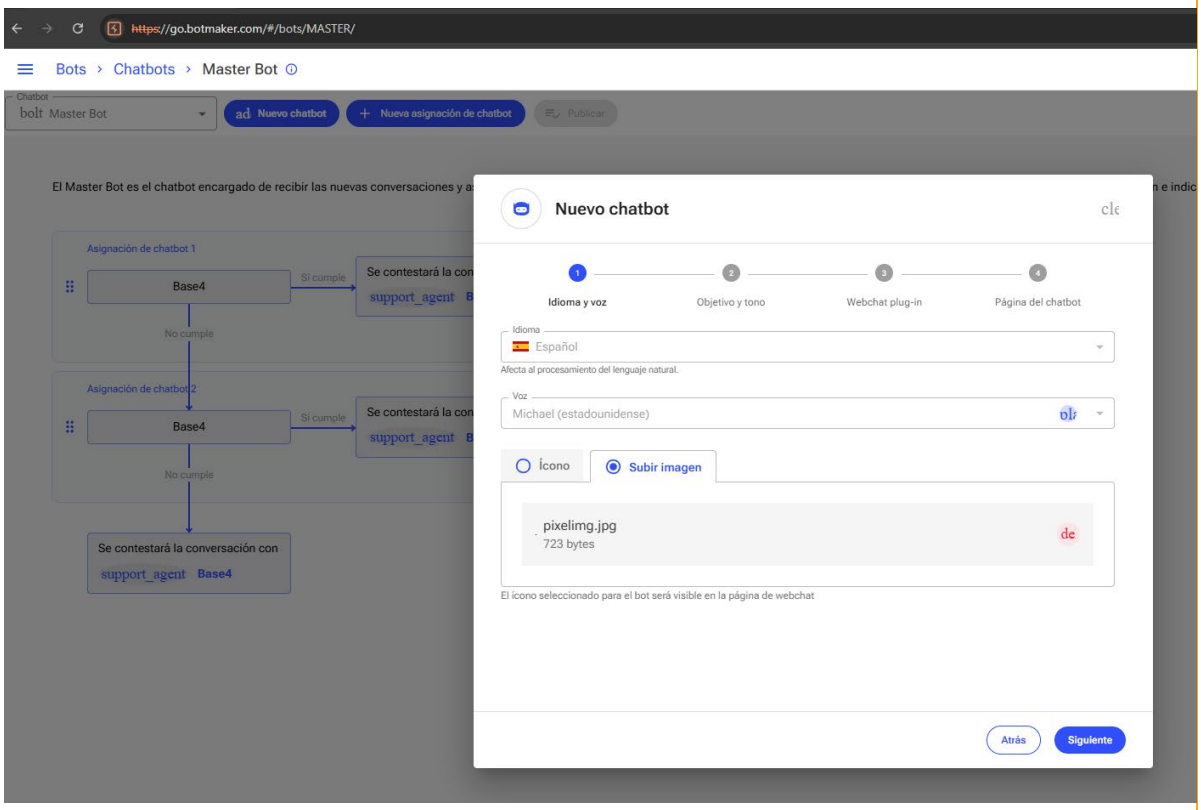
Vulnerabilidad

Se ha identificado una vulnerabilidad en el sistema de subida de archivos de la aplicación, que permite aceptar extensiones inseguras. Durante la prueba de concepto, se logró subir un archivo con extensión .html y ejecutar código **JavaScript** incrustado. Esto abre la posibilidad de que un atacante suba archivos maliciosos que se ejecuten automáticamente en los navegadores de las víctimas al acceder a la URL del archivo. La vulnerabilidad, asociada al manejo incorrecto de extensiones de archivos y la falta de validación de contenido, permite ataques como la ejecución de scripts maliciosos (XSS persistente) o incluso la inclusión de archivos maliciosos que podrían comprometer la integridad del sistema. Además, esta debilidad podría explotarse para lanzar ataques dirigidos, como phishing o propagación de malware. La falta de una lista blanca estricta para validar los archivos aceptados contribuye

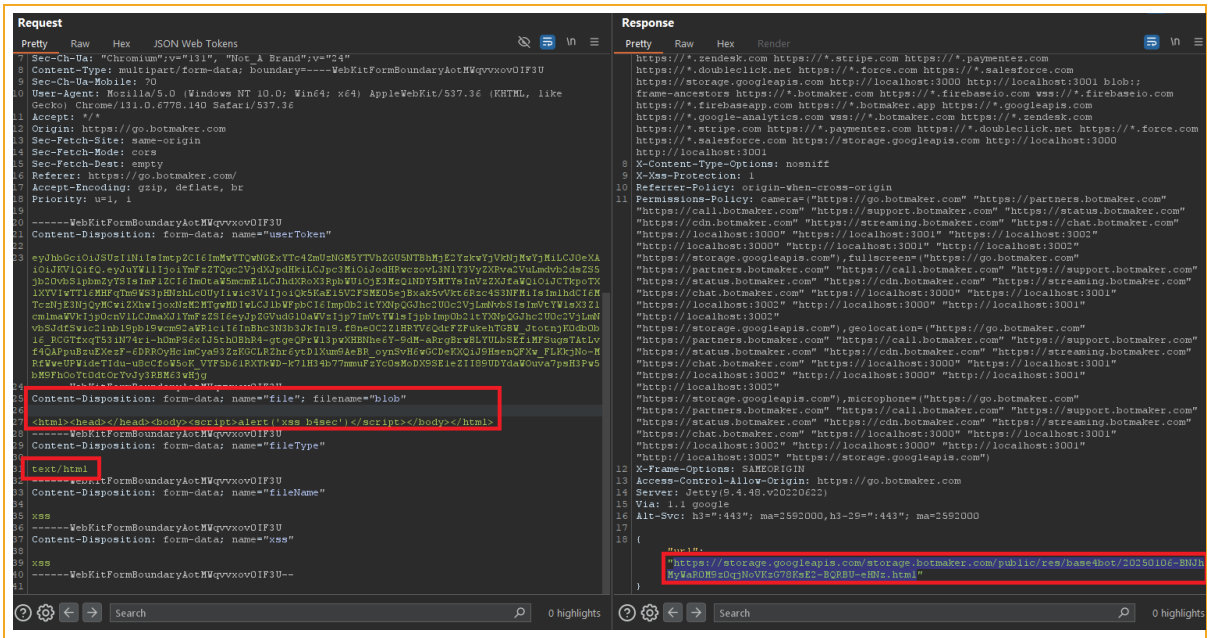
significativamente a la explotación de esta falla, afectando tanto la seguridad del servidor como de los usuarios finales.

Proceso y Evidencia

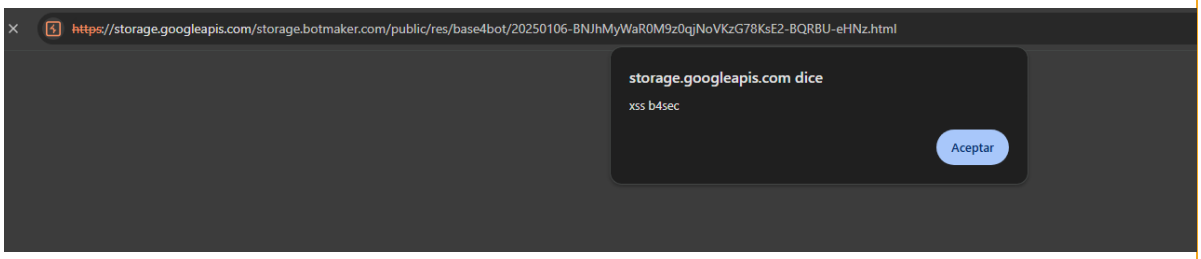
A través de la pantalla en el siguiente screenshot, se puede realizar la subida de archivos arbitraria:



En la siguiente imagen, se puede observar la request raw enviada al backend, donde al editar el content-type podemos determinar el tipo de archivo, en este caso vamos a decirle al back-end que estamos enviando un archivo tipo html, y que su contenido tiene el payload de nuestra prueba de concepto:



Ahora bien, si visitamos el link en cuestión, podemos ver la ejecución del alert:



De esta manera queda demostrada la vulnerabilidad

Impacto

La vulnerabilidad impacta en la seguridad de la información y la confianza del sistema. Desde la perspectiva de la confidencialidad, la capacidad de un atacante para ejecutar código arbitrario podría exponer datos sensibles almacenados o en tránsito. En términos de integridad, un atacante podría alterar la funcionalidad de la aplicación al ejecutar scripts maliciosos, afectando el comportamiento esperado del sistema y comprometiendo datos almacenados en la aplicación. El impacto se extiende también a los usuarios finales, exponiéndolos a riesgos de phishing, robo de credenciales y ataques dirigidos, lo que daña la confianza en la plataforma.

Recomendación

Se recomienda implementar una validación estricta de los archivos subidos utilizando una lista blanca que limite las extensiones permitidas exclusivamente a formatos

seguros como **.jpg y .png**. Es fundamental inspeccionar no solo las extensiones de los archivos, sino también sus firmas y contenido, para prevenir cargas maliciosas. Además, debe configurarse el servidor para que los directorios de archivos subidos no permitan la ejecución de scripts o código. Finalmente, habilitar un sistema de alertas que notifique intentos de cargar archivos con extensiones no permitidas ayudará a mitigar futuros intentos de explotación.

Referencias

Puede visitar los siguientes enlaces para más información:

- https://cwe.mitre.org/data/definitions/434.html
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html
- https://portswigger.net/web-security/file-upload

Re-Test

Se identificó una vulnerabilidad en el sistema de subida de archivos que permitía aceptar extensiones inseguras, como .html, y ejecutar código JavaScript incrustado al acceder al enlace del archivo. Esto exponía a la aplicación a riesgos como la ejecución de scripts maliciosos (XSS persistente) y posibles ataques dirigidos a los usuarios finales. Durante el retest, se verificó que los archivos con extensiones inseguras ya no se ejecutan automáticamente en el navegador, sino que se descargan como archivos estáticos. Esta medida mitiga el riesgo asociado al XSS persistente, y el hallazgo se considera mitigado:

Request

Pretty Raw Hex Hackvertor

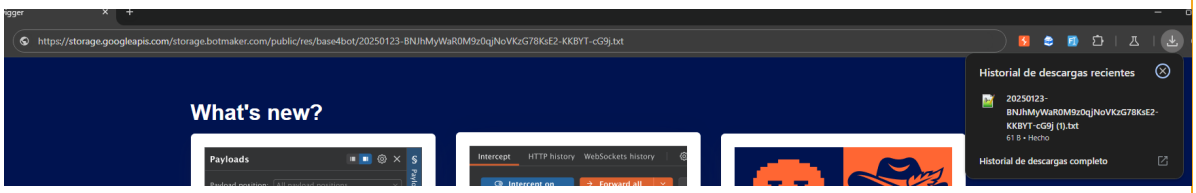
```
GET /storage.botmaker.com/public/res/base4bot/20250123-BNJhMyWaR0M9z0qjNoVKzG78KsE2-KKBYT-cG9j.txt HTTP/2
Host: storage.googleapis.com
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: es-ES,es;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
X-Client-Data: CJ31yqE=
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

Pretty Raw Hex Render Hackvertor

```
HTTP/2 200 OK
X-Guploader-Uploadid: AFIdbgSqmfFYnFdEdyvOzBJu-9s_lDpyco2Vg-UG5ACNFHqHSRcna29sQr4JvnaD6inui72U
X-Goog-Generation: 1737653570790225
X-Goog-Metageneration: 1
X-Goog-Stored-Content-Encoding: identity
X-Goog-Stored-Content-Length: 61
X-Goog-Meta-Bid: base4bot
Content-Disposition: attachment; filename="20250123-BNJhMyWaR0M9z0qjNoVKzG78KsE2-KKBYT-cG9j.txt
X-Goog-Hash: crc32c=qpZzfA==
X-Goog-Hash: md5=lBdS6njbrPnzVIzKOmopjQ==
X-Goog-Storage-Class: STANDARD
Accept-Ranges: bytes
Content-Length: 61
Access-Control-Allow-Origin: *
Server: UploadServer
Date: Thu, 23 Jan 2025 17:33:05 GMT
Expires: Fri, 23 Jan 2026 17:33:05 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Thu, 23 Jan 2025 17:32:50 GMT
Etag: "d41752ea78dbacf9f3548ccad26a298d"
Content-Type: text/html
Age: 33
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<script>
    window.location.href='https://base4sec.com';
</script>
```



A4. ServerSide Request Forgery (localhost bypass)

Descripción					
Activo(s) Afectado(s)	• https://ws.botmaker.com/stable10/ws/console/endpoint/				
Impacto	Medio	Probabilidad	Alto	Riesgo	Alto
CVE/CWE	CWE-918: Server-Side Request Forgery (SSRF) CWE-693: Protection Mechanism Failure		Mitigación	Mitigado	
OWASP	A10: Server-Side Request Forgery (SSRF)		Remediación	**Programación**	
CVSSv3.1	7.7				
Mitre ATT&CK	N/A				

Vulnerabilidad

Se ha identificado una vulnerabilidad en la funcionalidad de webhooks de la aplicación, en la cual las restricciones de acceso a localhost están implementadas exclusivamente en el front-end del portal. Este enfoque deja al sistema expuesto, ya que un atacante puede modificar el tráfico enviado a través del websocket para sortear estas restricciones. Como resultado, es posible realizar peticiones no autorizadas al servidor local (localhost), lo que puede desencadenar ataques de Server-Side Request Forgery (SSRF).

El ataque se facilita porque el sistema carece de un control efectivo en el backend que valide y restrinja las direcciones de destino de las solicitudes. Un atacante con experiencia puede interceptar las peticiones, alterar la dirección de destino hacia **127.0.0.1 o localhost** y ejecutar más allá de los límites establecidos, como acceder a servicios internos que no deberían ser accesibles desde el scope del usuario. Esto

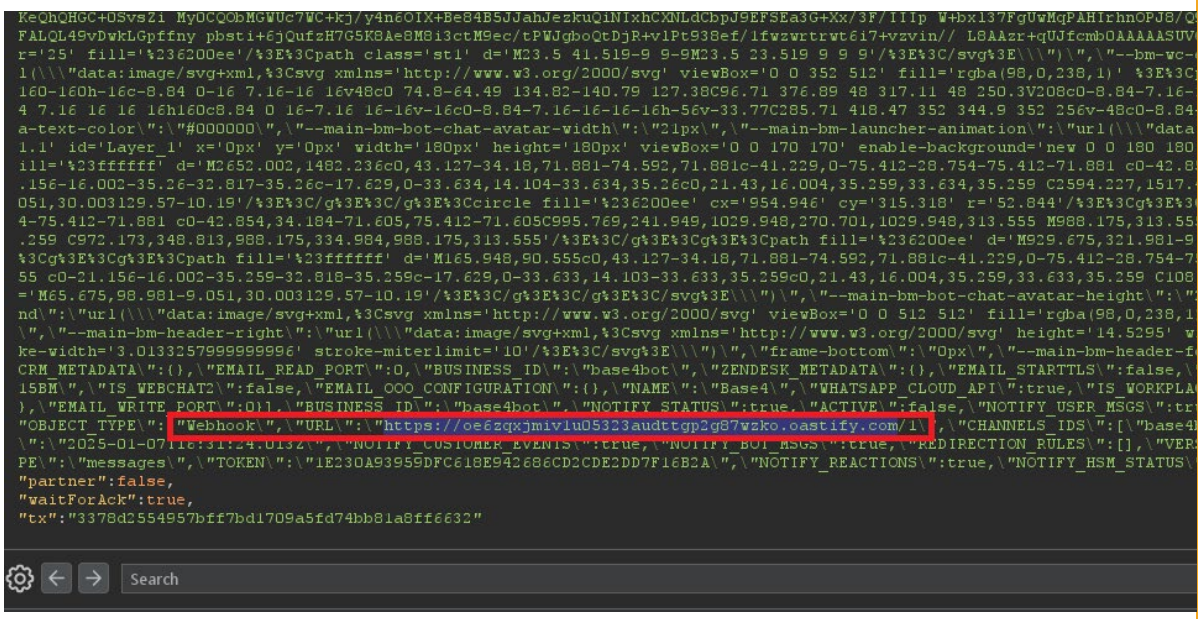
expone información sensible, como metadatos internos o configuraciones críticas, y permite ejecutar acciones potencialmente peligrosas en servicios vulnerables.

Proceso y Evidencia

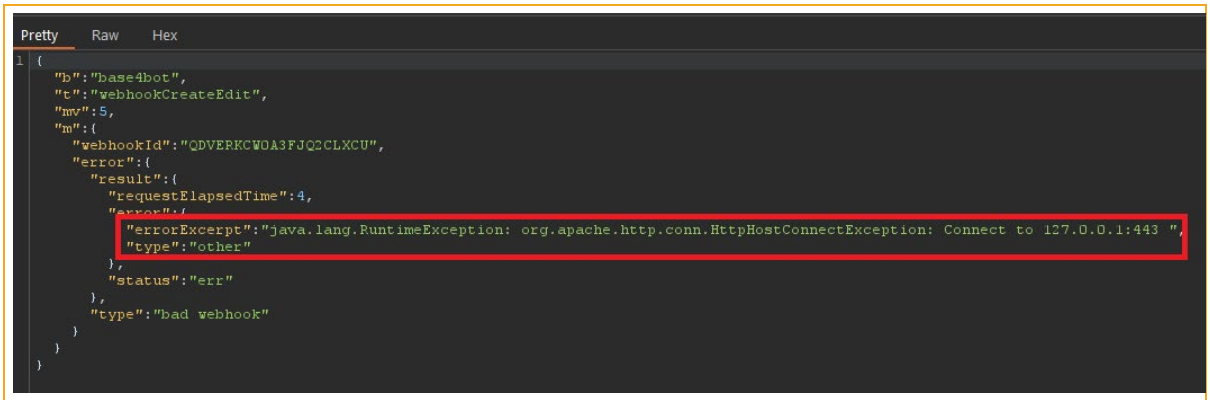
Durante la auditoría se detectó en la siguiente sección del sitio, que es posible realizar un bypass de los controles del front end:



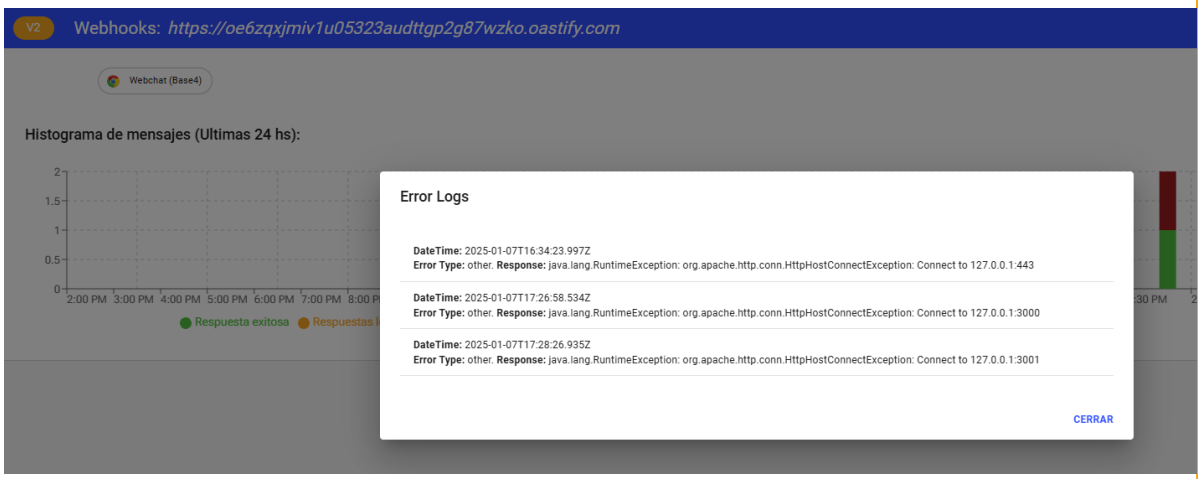
Sin embargo es posible modificar el tráfico en la comunicación del websocket y enviar un host arbitrario como por ejemplo **localhost**:



En este caso, se detecta que 443 en el host que envía la request no está disponible o no tiene un puerto abierto. Pero la request se realiza de manera exitosa saltando los controles que impiden enviar el formulario con un webhook en **localhost** ya que el error que se muestra a continuación nos indica que el puerto 443 en 127.0.0.1 no está disponible, el error observado a continuación, es equivalente a un Time Out:



Se han intentado además los puertos 3000 y 3001 ya que se observa en la cabecera **ContentSecurityPolicy** del servidor estas direcciones, sin embargo estos servicios, parecen ser también servicios de otro entorno no productivo y que no están disponibles en el entorno actual. Así mismo, un atacante que automatice esta práctica de enviar la data al websocket y luego inspeccionar los logs con los errores, podrá realizar escaneos http dentro de la red interna del activo afectado. A continuación se muestran los mensajes de error en los logs que confirman esto:



Impacto

Esta vulnerabilidad compromete, especialmente la confidencialidad del sistema. Al permitir a un atacante interactuar con servicios internos del servidor mediante ataques de SSRF, la vulnerabilidad expone información sensible almacenada en servicios internos que normalmente no son accesibles desde el exterior.

Por otro lado, al ser una vulnerabilidad que depende de controles insuficientes en el backend, el ataque puede ejecutarse sin alertar a los sistemas de monitoreo

tradicionales que confían únicamente en las restricciones del front-end. Esto dificulta la detección y la mitigación temprana del ataque, aumentando el riesgo de daños persistentes.

Recomendación

Recomendamos implementar validaciones de restricción de acceso a **localhost** en el backend de la aplicación. Esto incluye configurar reglas explícitas que bloqueen solicitudes a direcciones internas, como **127.0.0.1** o **::1**, y cualquier rango de IP (**127.1.1.1/8**) interno no autorizado. Además, se debe realizar una validación robusta de los encabezados y cuerpos de las solicitudes en el backend para asegurar que el destino permitido esté limitado a los dominios autorizados. Estas medidas deben complementarse con la activación de registros de auditoría que identifiquen intentos de explotación de esta vulnerabilidad y permitan responder a tiempo ante actividades sospechosas.

Referencias

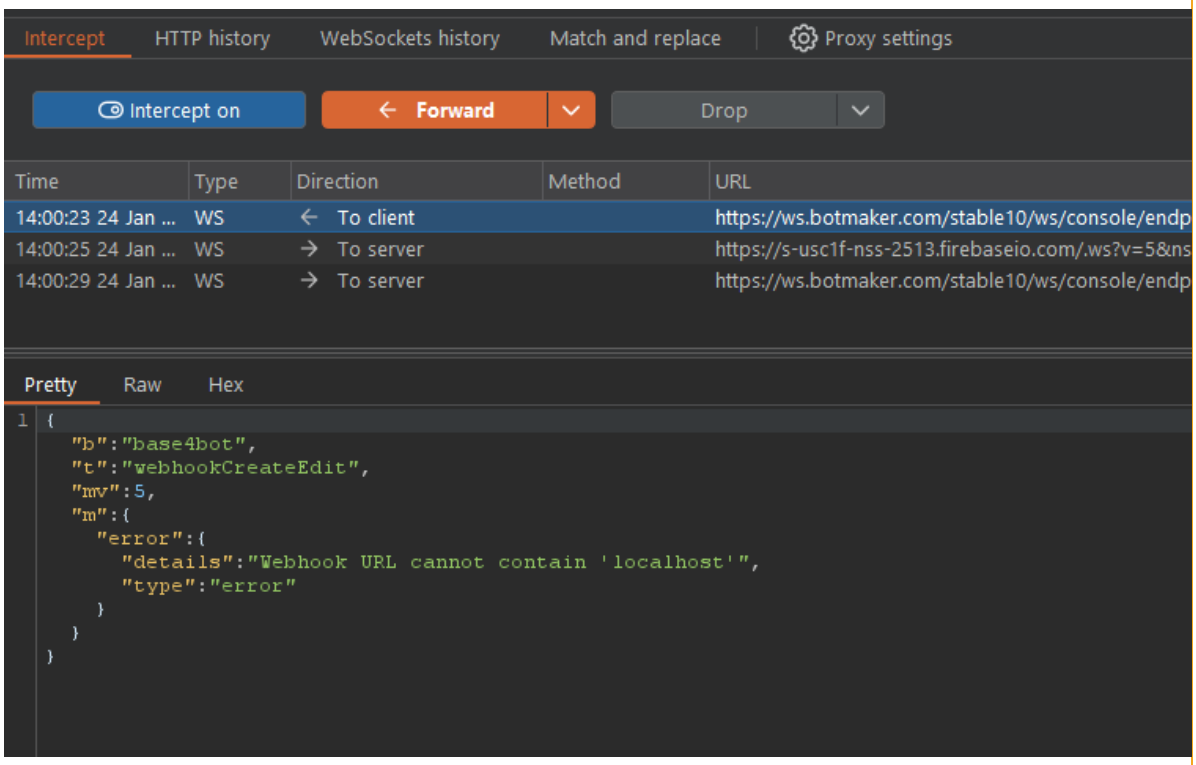
Puede visitar los siguientes enlaces para más información:

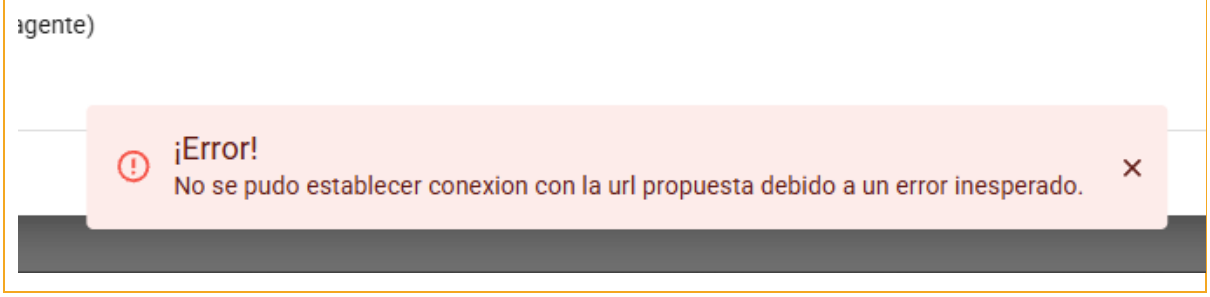
- https://owasp.org/www-community/attacks/Server_Side_Request_Forgery
- https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html
- https://cwe.mitre.org/data/definitions/918.html
- https://portswigger.net/web-security/ssrf

Re-Test

Se identificó una vulnerabilidad en la funcionalidad de webhooks, donde las restricciones de acceso a localhost estaban implementadas únicamente en el front-end, permitiendo a un atacante modificar el tráfico enviado a través del websocket para evadir dichas restricciones. Esto habilitaba ataques de **Server-Side Request Forgery (SSRF),** permitiendo realizar solicitudes no autorizadas a servicios internos en **127.0.0.1**, localhost y otras representaciones equivalentes. Durante el retest, se verificó que se ha implementado una validación robusta en el backend, que restringe de manera efectiva las direcciones de destino de las solicitudes. Además, se identificó que el filtro se ha fortalecido para incluir representaciones adicionales de localhost,

como **127.1**, mitigando completamente este riesgo. Este hallazgo se considera mitigado.





M1. Software Information Disclosure

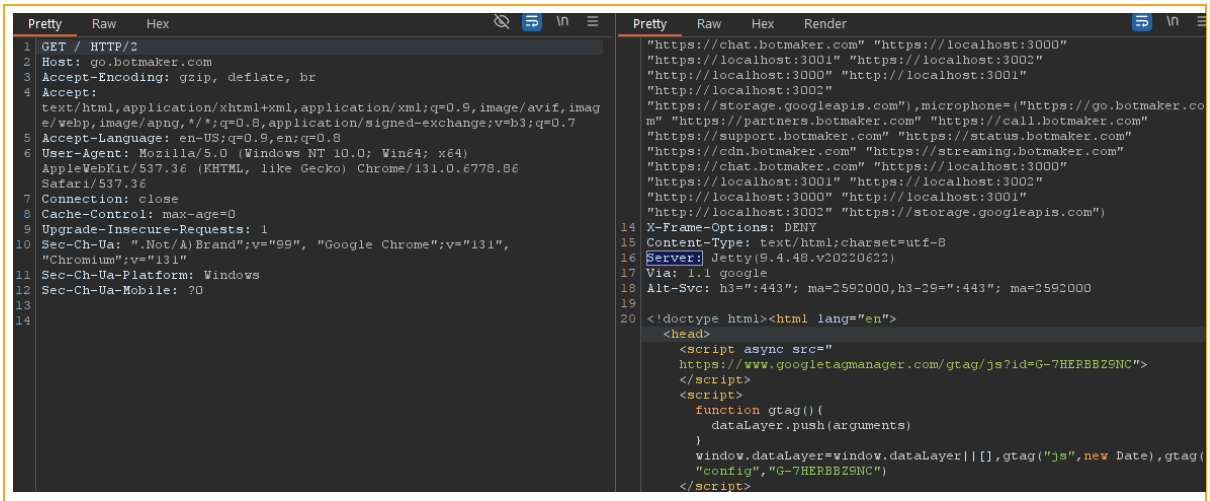
Descripción					
Activo(s) Afectado(s)	• https://go.botmaker.com/				
Impacto	Bajo	Probabilidad	Alta	Riesgo	Medio
CVE/CWE	CWE-200		Mitigación	Mitigado	
OWASP	A :2021-Security Misconfiguration		Remediación	**Configuración**	
CVSSv3.1	5.3				
Mitre ATT&CK	N/A				

Vulnerabilidad

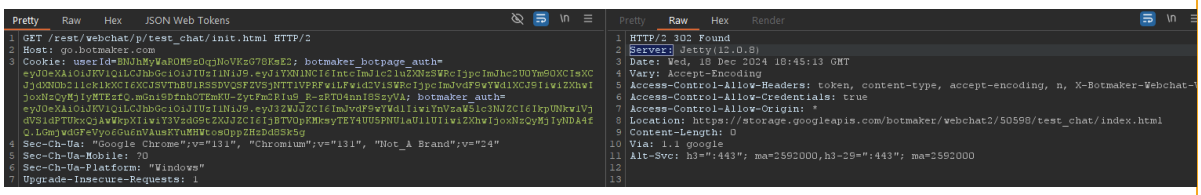
Se ha identificado que el servidor en cuestión expone versiones de software corriendo en el backend a través de sus cabeceras de respuesta. Esta exposición se da cuando el servidor comunica metadatos, a menudo como parte de su proceso estándar, que incluye detalles sobre los softwares y sus respectivas versiones. Aunque estas cabeceras están diseñadas para proporcionar información útil, en el contexto incorrecto, pueden ofrecer a los atacantes pistas valiosas sobre posibles vulnerabilidades presentes en el sistema. Especialmente si estas versiones son conocidas por tener vulnerabilidades no parcheadas. La determinación precisa de la versión de un software en uso puede allanar el camino para ataques dirigidos, donde un atacante puede explotar vulnerabilidades específicas de esa versión.

Proceso y Evidencia

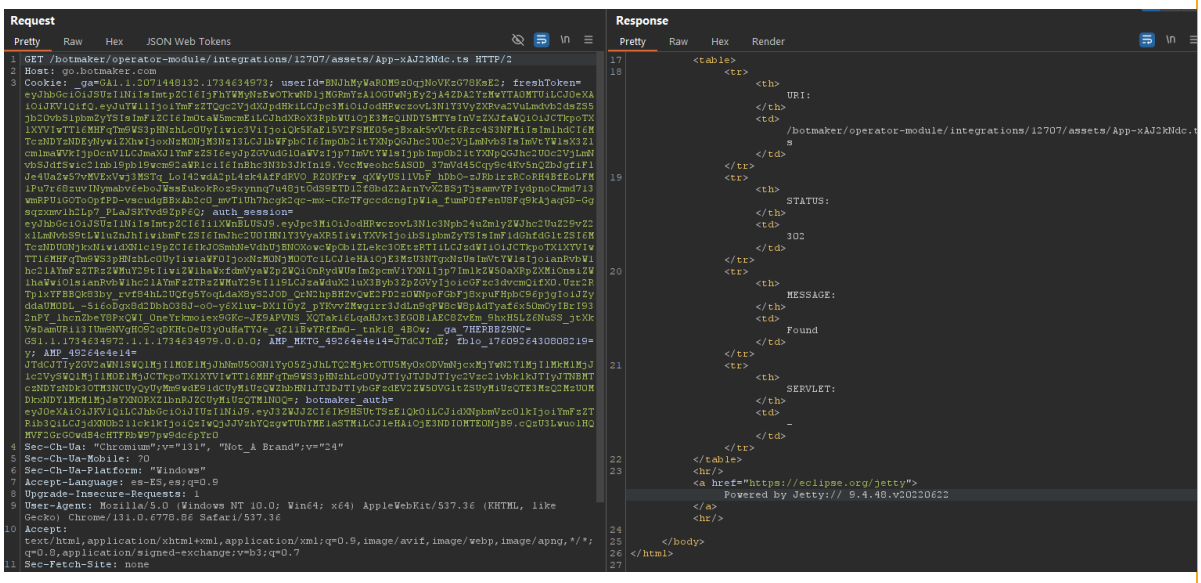
A través de la cabecera **"Server:"** se identificó que el sitio divulga la versión exacta de **Jetty**



Otro caso existe de iguales características, bajo el path **/rest/webchat/p/***



También el banner se puede ver al realizarse una redirección **302**:



Impacto

Al permitir que los atacantes identifiquen las versiones exactas del software en uso, se les otorga una ventaja significativa. Estos actores malintencionados pueden, con esta información, buscar y explotar vulnerabilidades conocidas asociadas a dichas versiones. Esta exposición puede conducir a ataques exitosos que resulten en el compromiso del sistema, pérdida de datos, interrupciones de servicio o incluso la infiltración en redes internas. Adicionalmente, la percepción de un ambiente no seguro puede afectar la confianza de los usuarios y clientes en la plataforma o servicio.

Recomendación

El primer paso para resolver esta vulnerabilidad es hardenizar el servidor web para que no exponga estas versiones de software.

1. Acceder a la configuración del servidor web.
2. Localizar las opciones de cabeceras de respuesta.
3. Desactivar o modificar las cabeceras que exponen versiones de software o cualquier otro detalle innecesario. O en su defecto si está utilizando proxies reversos, configure un filtro para que la cabecera no llegue al usuario final.

Referencias

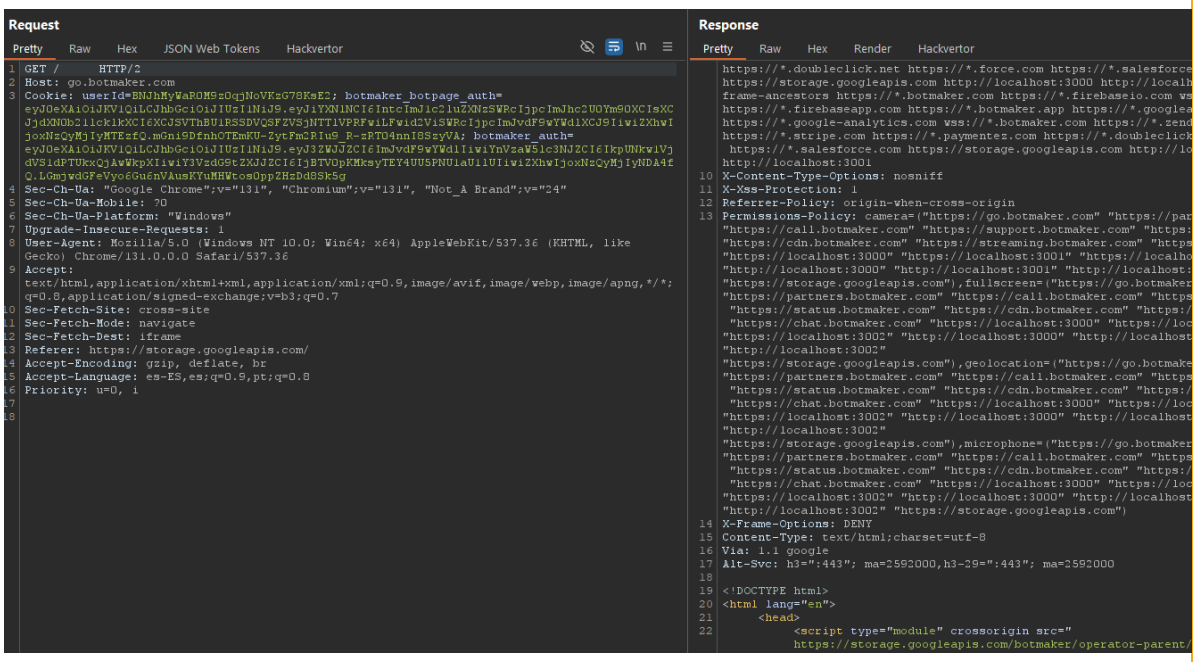
Puede visitar los siguientes enlaces para más información:

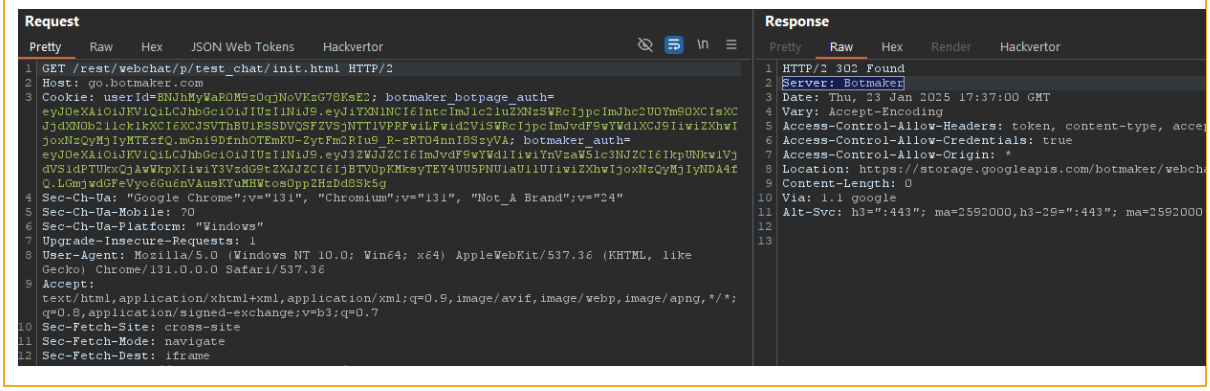
- https://cwe.mitre.org/data/definitions/200.html

Re-Test

Se identificó que el servidor expone versiones de software utilizadas en el backend a través de las cabeceras de respuesta **HTTP**. Esta práctica permitía a un atacante obtener detalles sobre los softwares y sus respectivas versiones, facilitando ataques dirigidos en caso de que dichas versiones fueran vulnerables. Durante el **retest**, se verificó que las cabeceras de respuesta han sido configuradas para omitir

información sobre los softwares y versiones utilizadas, eliminando las pistas que podrían ser explotadas. Este hallazgo se considera mitigado.





B1. Path Traversal: Acciones de Código

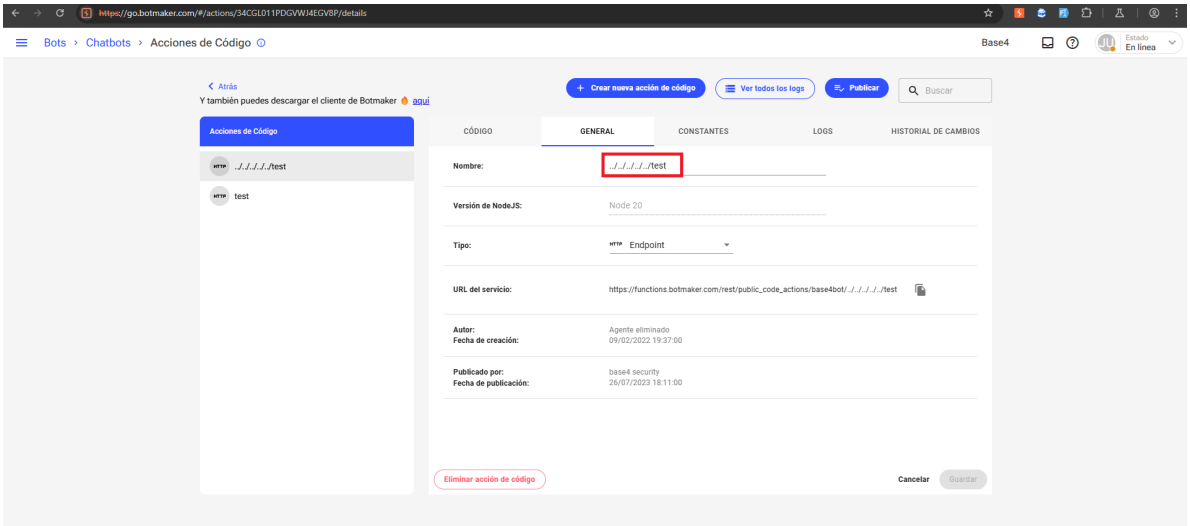
Descripción					
Activo(s) Afectado(s)	• https://go.botmaker.com/				
Impacto	Bajo	Probabilidad	Medio	Riesgo	Bajo
CVE/CWE	CWE-22: Path Traversal		Mitigación	Mitigado	
OWASP	TOP10:2021: A01 - Broken Access Control		Remediación	**Programación**	
CVSSv3.1	3.1				
Mitre ATT&CK	N/A				

Vulnerabilidad

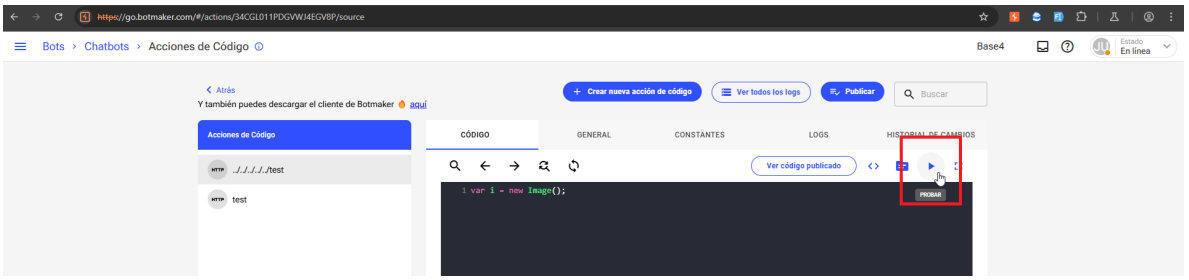
Se ha identificado una vulnerabilidad de tipo **Directory Traversal** en la sección de acciones de código dentro del subdominio functions. Durante la evaluación, se detectó que es posible manipular la URL configurando su nombre para incluir secuencias de retroceso de directorios (../). Esto sucede debido a la ausencia de una verificación robusta en el campo afectado, lo que permite a un atacante potencial eludir las restricciones de acceso y navegar fuera del directorio permitido. Este vector puede explotarse para ataques más sofisticados. Esta vulnerabilidad es susceptible de ser encadenada con otros vectores de ataque, como redirecciones arbitrarias, aumentando significativamente su impacto. La falta de validación adecuada convierte el campo afectado en un componente de éxito para ataques avanzados.

Proceso y Evidencia

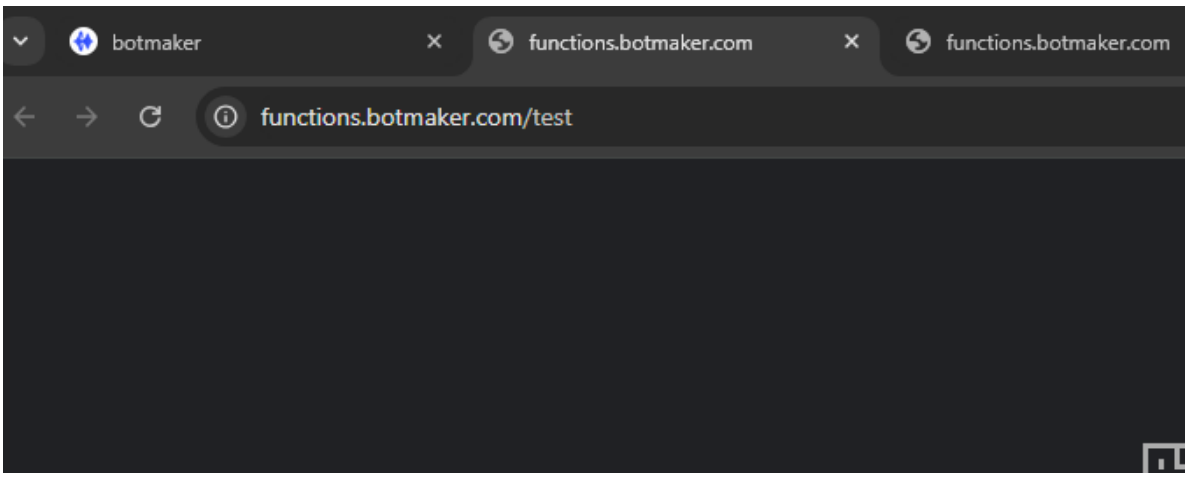
A continuación en la sección de Acciones de código podemos escapar el directorio de la siguiente manera:



Para ejecutar el escape en un solo click, podemos ingresar desde el siguiente ícono:



De esta manera podemos confirmar el escape del directorio del usuario:



Impacto

Esta vulnerabilidad afecta la integridad. Un atacante puede escapar del directorio donde está permitido operar, poniendo en riesgo la integridad, un atacante podría utilizar este vector para llegar a funciones o endpoints fuera del scope del directorio, alterando el comportamiento del sistema.

Recomendación

Se recomienda implementar una validación estricta en el servidor para evitar que los usuarios puedan incluir secuencias de retroceso de directorios (../) en los campos afectados. Esto puede lograrse eliminando dichas secuencias en el procesamiento de la entrada del usuario y asegurándose de que los nombres de archivo o rutas se limiten únicamente a directorios autorizados.

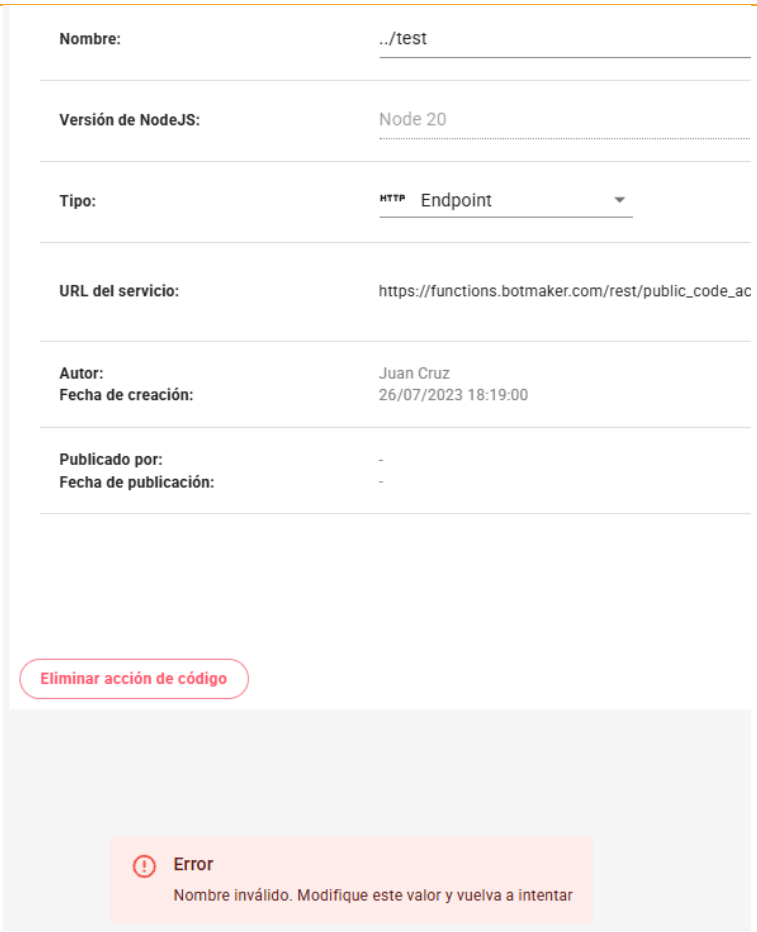
Referencias

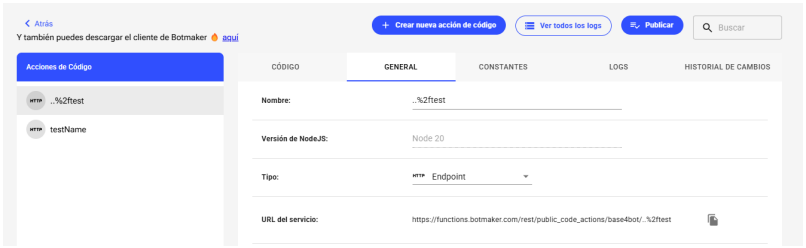
Puede visitar los siguientes enlaces para más información:

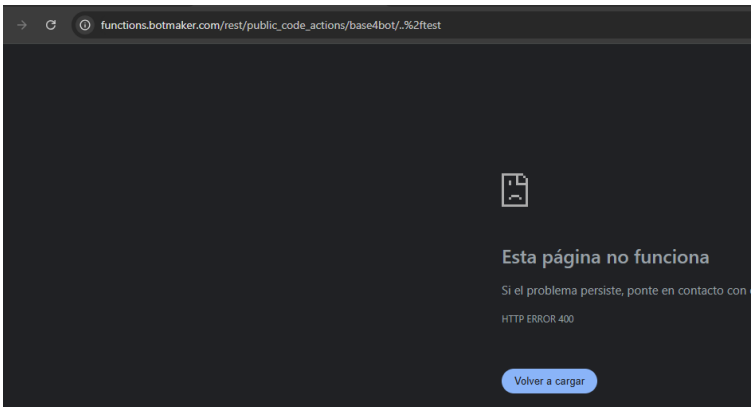
- https://owasp.org/www-community/attacks/Path_Traversal
- https://cwe.mitre.org/data/definitions/22.html
- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Re-Test

Se identificó una vulnerabilidad de tipo **Directory Traversal** en la sección de acciones de código del subdominio functions, que permitía la manipulación de la **URL** mediante secuencias de retroceso de directorios (../). Esto exponía al sistema a la posibilidad de eludir restricciones de acceso y navegar fuera del directorio permitido, incrementando el riesgo de ataques encadenados con otros vectores. Durante el retest, se verificó que se han implementado controles robustos para validar las entradas del campo afectado, bloqueando cualquier intento de navegación fuera del directorio permitido. Este hallazgo se considera mitigado.


Nombre:
../test
Versión de NodeJS:
Node 20
Tipo:
HTTP Endpoint
URL del servicio:
https://functions.botmaker.com/rest/public_code_ac
Autor:
Juan Cruz
Fecha de creación:
26/07/2023 18:19:00
Publicado por:
-
Fecha de publicación:
-
Eliminar acción de código
Error
Nombre inválido. Modifique este valor y vuelva a intentar


Atrás
Y también puedes descargar el cliente de Botmaker aquí
Crear nueva acción de código
Ver todos los logs
Publicar
Buscar
Acciones de Código
..%2ftest
testName
CÓDIGO
GENERAL
CONSTANTES
LOGS
HISTORIAL DE CAMBIOS
Nombre:
..%2ftest
Versión de NodeJS:
Node 20
Tipo:
HTTP Endpoint
URL del servicio:
https://functions.botmaker.com/rest/public_code_actions/base4bot/..%2ftest


functions.botmaker.com/rest/public_code_actions/base4bot/..%2ftest
Esta página no funciona
Si el problema persiste, ponte en contacto con
HTTP ERROR 400
Volver a cargar

Conclusión

Dadas las vulnerabilidades revisadas durante la ejecución del **Re-Test del Pentest Web** a los activos indicados por **BotMaker**, se concluyó que los activos analizados poseen un nivel de seguridad **Alto**.

Durante las pruebas de seguridad realizadas sobre el aplicativo web, se identificaron un total de seis (6) vulnerabilidades clasificadas en distintos niveles de riesgo: **Alto**, **Medio** **y** **Bajo.** Cada una de estas vulnerabilidades representaba un riesgo significativo para la seguridad del sistema, con potencial de comprometer la confidencialidad, integridad o disponibilidad del entorno.

A través del proceso de mitigación y el posterior retest, se ha confirmado que todas las vulnerabilidades identificadas han sido completamente abordadas, implementando controles efectivos que eliminan los riesgos asociados. Las medidas correctivas aplicadas incluyen la implementación de validaciones robustas, ajustes en las configuraciones de seguridad del servidor y actualizaciones de los componentes del sistema afectados. Estas acciones han eliminado las posibilidades de explotación de los vectores de ataque previamente detectados.

El aplicativo web ahora cuenta con un entorno fortalecido frente a las amenazas identificadas, asegurando que los riesgos reportados han sido mitigados en su totalidad. Este resultado refleja el compromiso del equipo de desarrollo con la seguridad del sistema y la protección de sus usuarios, garantizando un entorno seguro y confiable.

Al contratar los servicios profesionales de **Base4 Security** para la ejecución de un **Pentest Web, BotMaker** se ha adelantado a los hechos en forma proactiva; ya que estas fallas de seguridad pueden ser identificadas y explotadas por un actor malicioso y así comprometer la confidencialidad, integridad y disponibilidad de sus sistemas. Se recomienda revisar el informe técnico con las áreas pertinentes del negocio para

evaluar la mitigación de las vulnerabilidades halladas, fortaleciendo así aún más la postura de seguridad de la organización.

Proceso de Pentest Web

Las pruebas realizadas en un **Pentest Web** difieren de los escaneos automatizados de vulnerabilidades, ya que las primeras son exhaustivas y buscan explotar las vulnerabilidades identificadas con el objetivo de reproducir un escenario real de ataque realizado por un posible adversario.

Cuando se trata de aplicaciones web críticas, es apropiado realizar una revisión detallada. Dado que las aplicaciones web varían ampliamente en términos de propósito, función, arquitectura y base de código, los enfoques específicos, las perspectivas de prueba y los perfiles de prueba utilizados pueden variar.

El enfoque de **Base4 Security** para las pruebas de intrusión de aplicaciones web proporciona un marco flexible para identificar y evaluar exhaustivamente las vulnerabilidades técnicas.

Todas estas pruebas siguen los estándares detallados a continuación:

OWASP Web Security Testing Guide

OWASP Web Security Testing Guide (WSTG) es una guía completa para probar la seguridad de las aplicaciones web y los servicios web. Cubre una amplia gama de grupos de prueba para ayudar a garantizar que las aplicaciones web sean seguras. A continuación, se describen cada uno de los grupos de pruebas.

Recopilación de información

Este grupo de pruebas se enfoca en recopilar información sobre la aplicación web que podría usarse para explotar vulnerabilidades. Esta información puede incluir la dirección IP de la aplicación, el nombre de host, el sistema operativo, el software del servidor web y el marco de la aplicación.

Pruebas de gestión de configuración e implementación

Este grupo de pruebas se centra en la configuración y la implementación de la aplicación web. Esto incluye pruebas de configuraciones inseguras, como contraseñas débiles, puertos abiertos y software obsoleto.

Pruebas de gestión de identidad

Este grupo de pruebas se centra en los mecanismos de identificación de los usuarios. Comprende pruebas como enumeración de usuarios, aprovisionamiento de cuentas, identificadores de usuario predecibles, entre otras.

Pruebas de autenticación

Este grupo de pruebas se centra en los mecanismos de verificación de la identidad del usuario. Comprende pruebas como mecanismos de autenticación débil, evasión del esquema de autenticación, mecanismos de recuperación de claves, políticas de contraseñas, múltiples factores de autenticación, etc.

Pruebas de autorización

Este grupo de pruebas se centra en los mecanismos de control de acceso a las funciones de la aplicación. Comprende pruebas como evasión del esquema de autorización, referencia insegura y directa a objetos, escalamiento de privilegios, etc.

Pruebas de gestión de sesiones

Este grupo de pruebas se centra en los mecanismos de gestión de sesiones de la aplicación web. Esto incluye pruebas de fijación de sesiones, secuestro de sesiones y falsificación de solicitudes entre sitios (CSRF).

Pruebas de validación de entrada

Este grupo de pruebas se centra en los mecanismos de validación de entrada de la aplicación web. Esto incluye pruebas de inyección SQL, secuencias de comandos entre sitios (XSS) e inyección de comandos.

Pruebas de manejo de errores

Este grupo de pruebas se enfoca en los mecanismos de manejo de errores de la aplicación web. Esto incluye la prueba de mensajes de error que podrían usarse para explotar vulnerabilidades.

Pruebas de criptografía débil

Este grupo de pruebas se centra en los mecanismos de criptografía de la aplicación web. Esto incluye pruebas de algoritmos débiles, claves inseguras e implementación incorrecta.

Pruebas de lógica de negocio

Este grupo de pruebas se centra en la lógica del negocio de la aplicación web. Esto incluye pruebas de vulnerabilidades que podrían ser aprovechadas por atacantes para obtener acceso no autorizado a datos o sistemas.

Pruebas del lado del cliente

Este grupo de pruebas se centra en los componentes del lado del cliente de la aplicación web. Esto incluye pruebas de vulnerabilidades en JavaScript, HTML y CSS.

OWASP Top 10 - 2021

A01:2021 – Pérdida de Control de Acceso

Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades, datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar permisos de acceso, etc.

A02:2021 – Fallas Criptográficas

Muchas aplicaciones web y APIs no protegen adecuadamente los datos sensibles tales como información financiera, de salud o Información Personal Identificable (PII). El mal uso de la criptografía o la falta de uso de esta conduce a menudo a la exposición de datos sensibles. Se debe determinar las necesidades de protección de los datos en tránsito y en reposo.

A03:2021 – Inyección

Las fallas de inyección ocurren cuando se envían datos no confiables a un intérprete como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización. Algunas vulnerabilidades de inyección son: inyección SQL, inyección LDAP, inyección XML, etc.

A04:2021 – Diseño Inseguro

Engloba múltiples vulnerabilidades que se caracterizan por tener su origen en la falta o el diseño incorrecto de controles de seguridad durante las etapas tempranas del desarrollo de software. A diferencia de las vulnerabilidades debidas a implementaciones inseguras, este tipo de vulnerabilidades no se resuelven mejorando la codificación puesto que el software es vulnerable por diseño.

A05:2021 – Configuración de Seguridad Incorrecta

El software utilizado actualmente se caracteriza por ser altamente configurable. Muchas de estas opciones de configuración vienen con valores predefinidos pensados para una puesta en marcha rápida. Sin embargo, las configuraciones por defecto, por lo general no son las más seguras e incluso pueden representar brechas de seguridad graves. Algunos ejemplos de configuración de seguridad incorrecta son: falta de hardening, funcionalidades innecesarias habilitadas, credenciales por defecto habilitadas, ejecución en modo debug, etc.

A06:2021 – Componentes Vulnerables y Desactualizados

Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.

A07:2021 – Fallas de Identificación y Autenticación

Las funciones relacionadas a la identificación, autenticación y gestión de la sesión del usuario son esenciales para la seguridad de las aplicaciones. Algunos fallos comunes en esta categoría son: vulnerabilidades de enumeración de usuarios, permitir realizar ataques de fuerza bruta o password spraying, exponer el identificador de sesión en la URL, no invalidar correctamente el identificador de sesión luego del cierre, etc.

A08:2021 – Fallas en la Integridad del Software y Datos

Estos fallos están relacionados con software e infraestructura no protegidos contra alteraciones. Por ejemplo, cuando el software utiliza librerías o módulos provenientes de repositorios o redes de entrega de contenido (CDN) no confiables o que puedan haber sido alterados. Otro caso es cuando las aplicaciones deserializan datos provenientes de fuentes inseguras o manipulables por los usuarios.

A09:2021 – Fallas en el Registro y Monitoreo

El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos.

A10:2021 – Falsificación de Solicitudes de Lado del Servidor

Las fallas de falsificación de solicitudes de lado del servidor (SSRF) ocurren cuando una aplicación obtiene un recurso remoto sin validar adecuadamente la URL del recurso provista por el usuario. El atacante puede forzar a la aplicación a enviar solicitudes maliciosas a destinos inesperados. La gravedad de esta vulnerabilidad aumenta en arquitecturas en la nube debido a la variedad y complejidad de los servicios.

Apéndices

Metodologías y Estándares Utilizados

Para el desarrollo de este servicio se hizo uso de las siguientes metodologías y estándares internacionales, las cuales brindan el marco de referencia y aseguran que se contemplen la totalidad de los aspectos relevantes para cada área de revisión y brindan adicionalmente una guía de las tareas específicas para el desarrollo del proyecto:

ISO/IEC 27002
Proporciona directrices y mejores prácticas para la gestión de la seguridad de la información, abarcando aspectos como la gestión de riesgos, controles de seguridad y la implementación de un sistema de gestión de la seguridad de la información (SGSI)

NIST SP-800-115 (Technical Guide to Information Security Testing and Assessment)
Proporciona orientación sobre la realización de diversas actividades de pruebas y evaluaciones de seguridad, incluyendo pruebas de penetración, evaluaciones de vulnerabilidades y evaluaciones de controles de seguridad. La guía describe un enfoque estructurado para estas actividades y abarca la planificación, ejecución, análisis e informes.

PCI-DSS (Payment Card Industry Data Security Standard)
Conjunto de estándares de seguridad que establece requisitos y medidas para proteger la información de tarjetas de pago, con el objetivo de prevenir el fraude y asegurar la integridad de los datos de los titulares de tarjetas durante las transacciones.

OSSTMM (Open Source Security Testing Methodology Manual)
Estándar de pruebas de seguridad de código abierto que proporciona un enfoque sistemático y estructurado para evaluar y medir la efectividad de los controles de seguridad en sistemas, redes y aplicaciones.

OWASP WSTG (Web Security Testing Guide)

Guía exhaustiva que proporciona un enfoque detallado y práctico para evaluar y mejorar la seguridad de las aplicaciones web, incluyendo metodologías, técnicas y herramientas recomendadas para llevar a cabo pruebas exhaustivas y efectivas.

OWASP ASVS (Application Security Verification Standard)

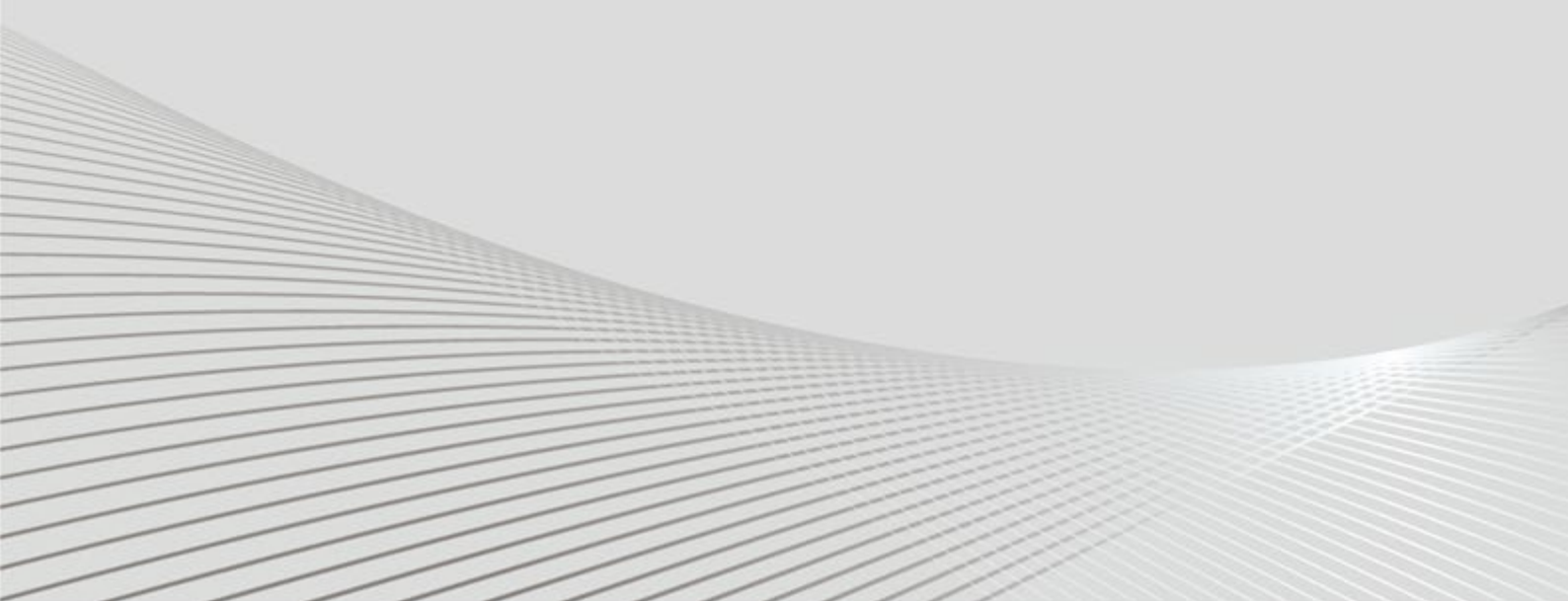
Guía de referencia que establece un conjunto de requisitos y controles de seguridad para evaluar y verificar la seguridad de las aplicaciones, cubriendo desde el diseño y desarrollo hasta la implementación y pruebas, con el objetivo de garantizar una postura de seguridad sólida.

MITRE ATT&CK

Marco de trabajo de ciberseguridad que describe y organiza tácticas, técnicas y procedimientos utilizadas por los adversarios en los ataques informáticos.

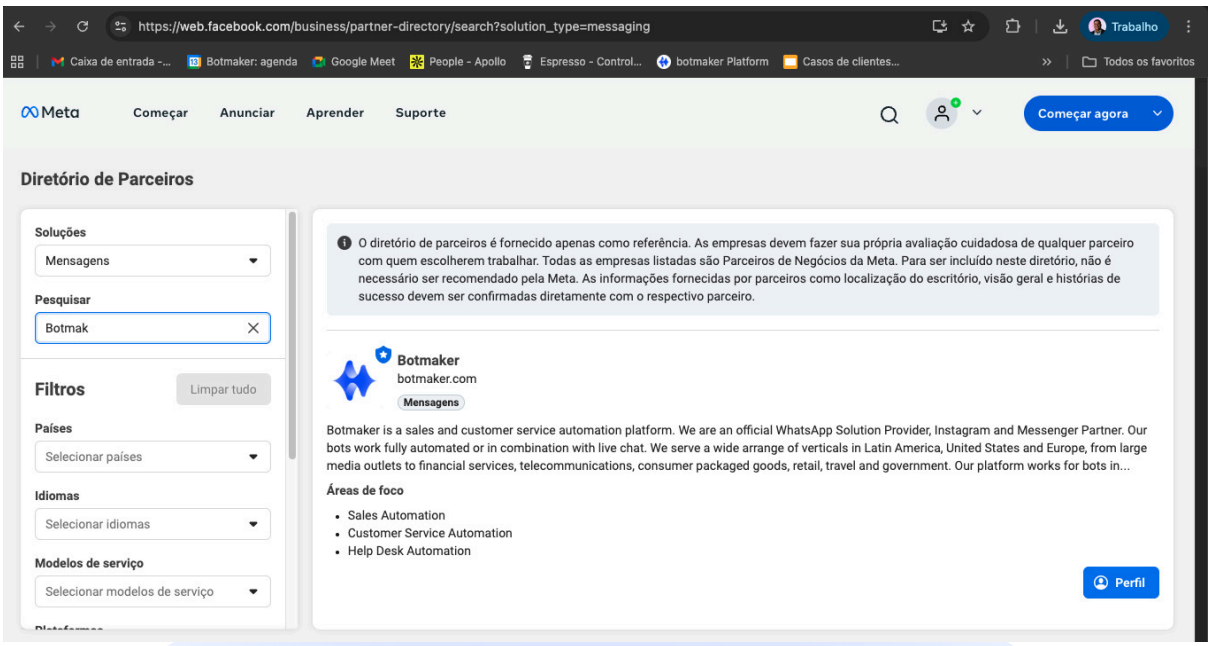
BASE4
SECURITY

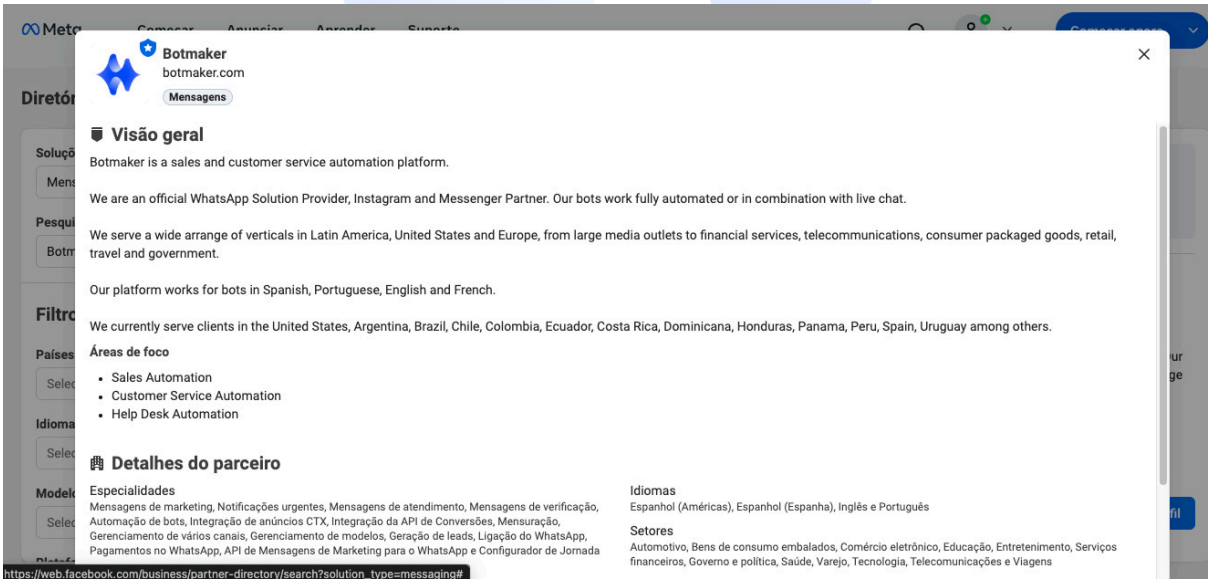
www.base4sec.com



botmaker
UNLEASH HUMAN POTENTIAL

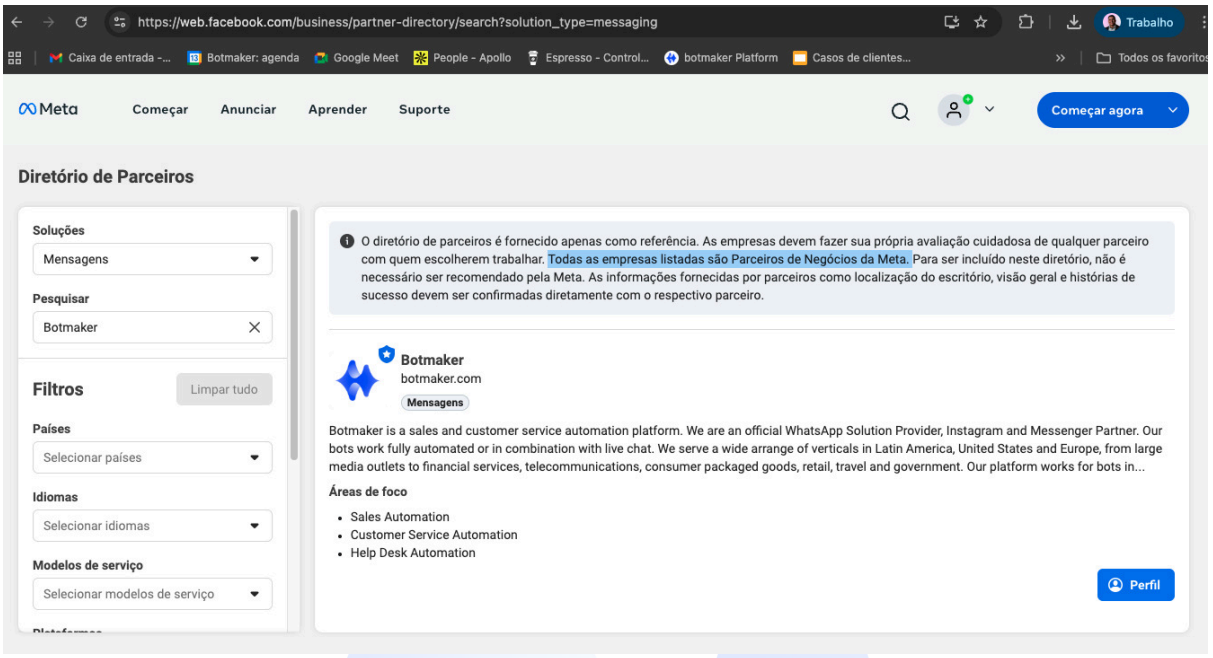
Comprovação Repositório Partners da META

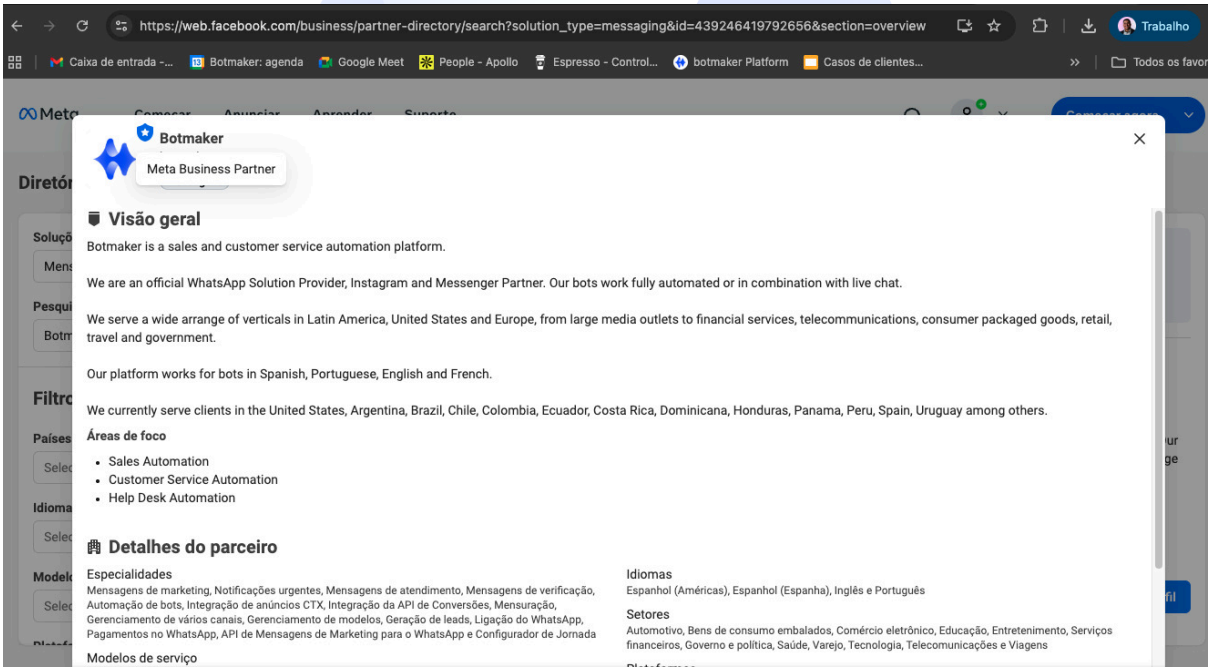




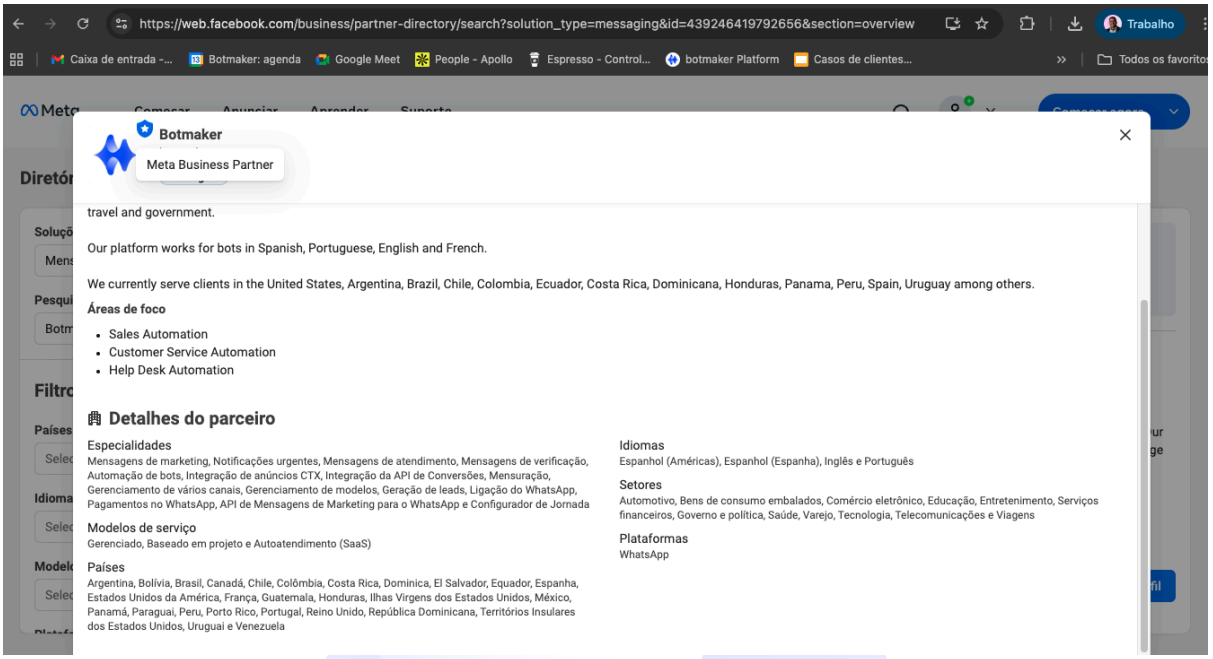
Clicksign 8d67c1f5-5246-4c83-ba58-e7cd26d95f6a

botmaker
UNLEASH HUMAN POTENTIAL





botmaker
UNLEASH HUMAN POTENTIAL



BM Brasil Internet Ltda

CNPJ: 30.607.960/0001-85

Felipe David Cohen
Diretor Financeiro

21 - COMPROVAÇÃO BUSINESS PARTNER META.pdf

Documento número #8d67c1f5-5246-4c83-ba58-e7cd26d95f6a

Hash do documento original (SHA256): df2e184b844005cf07a3e51122e5d0d8529020b92d1b876bc6d214cd9c9ce9a2

Assinaturas

Felipe Cohen
Assinou como representante legal em 24 nov 2025 às 09:01:25

Log

24 nov 2025, 07:43:40	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 criou este documento número 8d67c1f5-5246-4c83-ba58-e7cd26d95f6a. Data limite para assinatura do documento: 24 de dezembro de 2025 (07:42). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
24 nov 2025, 07:47:11	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Data limite para assinatura do documento: 24 de novembro de 2025 (16:00).
24 nov 2025, 07:47:11	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Finalização automática após a última assinatura: não habilitada.
24 nov 2025, 07:47:12	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 adicionou à Lista de Assinatura: felipe.cohen@botmaker.io para assinar como representante legal, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Felipe Cohen.
24 nov 2025, 09:01:25	Felipe Cohen assinou como representante legal. Pontos de autenticação: Token via E-mail felipe.cohen@botmaker.io. IP: 177.26.232.98. Localização compartilhada pelo dispositivo eletrônico: latitude -23.57810579346322 e longitude -46.6923699186964. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1346.2 disponibilizado em https://app.clicksign.com.
24 nov 2025, 09:16:46	Operador com email stephanie@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 finalizou o processo de assinatura. Processo de assinatura concluído para o documento número 8d67c1f5-5246-4c83-ba58-e7cd26d95f6a.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 8d67c1f5-5246-4c83-ba58-e7cd26d95f6a, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

Audit Report

SOC2 Type 2

Brief Description

Independent Auditor´s Report on Controls at a Service Organization relevant to Security, Integrity, Availability, and Confidentiality

Final version

Confidentiality Level

All information contained in this document must be kept strictly confidential, it is prohibited to copy and reproduce this document or part of it without the proper authorization of SIRYS S.R.L. The aforementioned obligations will remain in force even after their expiration or termination of use of this document.

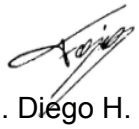
Buenos Aires, January 25th, 2025

Botmaker

Attn. Hernán Liendo

I am pleased to present the final version of the Independent Auditor's Report on Controls at a Service Organization relevant to Security, Integrity, Availability, and Confidentiality.

Sincerely,



Eng. Diego H. Fojo
SIRYS S.R.L.

Index

1. Purpose 3
2. Scope 3
3. Audit Criteria 3
4. Audit Team 3
5. Executive Summary 4
6. SECTION I – General Audit Conclusions 5
7. SECTION II - Security, Availability and Confidentiality Trust Service Principles, Applicable Criteria and Related Controls 8

1. Purpose

Analyze the existence of security, integrity, availability and confidentiality controls associated with the service offered through the "Botmaker Platform" in the SaaS modality and the internal services of "**Administration, operational support and maintenance of the service infrastructure**".

2. Scope

The scope of the audit is limited to the service offered through the **"Botmaker Platform"** in the SaaS modality and the internal services of **"Administration, operational support and maintenance of the service infrastructure"**.

The controls related to security, availability, processing integrity, confidentiality, and privacy of the information managed or associated with the service provided by the organization to its customers have been evaluated.

The evaluated service components are categorized into the following five areas:

- **Infrastructure**: The physical structures, IT and other hardware (e.g., facilities, computers, equipment, mobile devices and telecommunications networks).
- **Software**: The application programs and IT system software that support application programs (operating systems, middleware and utilities).
- **People**: The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel and managers).
- **Processes**: The automated and manual procedures.
- **Data**: Transaction flows, files, databases, tables and results used or processed by a system.

3. Audit Criteria

The audit and its corresponding report consider the Trust Services Principles (TSP) Section 100 of the American Institute of Certified Public Accountants (AICPA) as a reference framework to guide the audit criteria.

4. Audit Team

Eng. Diego H. Fojo

5. Executive Summary

Based on the review of the design and evidence of compliance with security controls, it was concluded that the organization satisfactorily meets these requirements, demonstrating a strong commitment to continuous improvement.

Additionally, the organization continuously manages its Information Security Management System (ISMS), certified under ISO/IEC 27001. This certification, maintained and renewed, demonstrates a strong commitment to information security, with the system's design including additional controls beyond those required in this report.

The organization has its own information security risk management methodology, which is continually refined through the management of security incidents and contributes to the ongoing improvement of security controls, as previously mentioned.

Section I below outlines the general conclusions based on the findings from the audit of control designs and the review of their evidence. Section II then provides detailed information on the design of each control defined in this report, along with the evidence of compliance that has been verified.

6. SECTION I – Audit General Conclusions

The controls relevant to the security, availability, and processing integrity, as well as the confidentiality and privacy of the information managed or associated with the service provided by the organization to its client, were evaluated.

The conclusions regarding the components of the evaluated service are as follows:

❖ Infrastructure

From an infrastructure perspective, the organization maintains physical locations that support the execution of services. However, the majority of personnel work remotely from their homes, meaning that contingencies affecting office buildings do not impact service delivery.

The physical infrastructure supporting the provision of the service is provided by Google Cloud, which ensures compliance with the highest standards, including ISO 27001, SOC 2, and others.

There is high availability of services and zone redundancy. Likewise, the following network security tools are in place:

- High Service Availability
- Zone Redundancy
- Google Cloud physical and equipment security
- Firewall, VPN devices
- Secure authentication via IAM
- Data storage and backup in the cloud.
- Notebooks designated for each staff.
- VPN tunneling infrastructure for access to critical infrastructure.

❖ Software

The organization has installed the necessary software for the daily operation of the service.

The support software, such as source code repository, code versioning, ticketing system, etc. are contracted in the SaaS modality to first level vendors.

❖ People

The organization has a hierarchical structure for service management, risk escalation and decision making.

The expertise of the personnel assigned to each function has been validated. Personnel undergo periodic training aligned with both their professional needs and the services they manage.

The number of professionals assigned to the services is determined based on the organization's needs, client requirements, and contractual guidelines.

❖ Procedures

The Organization has policies and guidelines regarding information security, including, among others:

- Framework Policy
- Specific Security Policies
- Logical Access Management
- Access Profiles
- Change Management
- Security Incident Management
- Organizational Chart and Job Profiles
- Risk Management
- Human Capital Management
- Training and Awareness
- Supplier Management
- Documented Information Management
- Environment Management:
    - Deployment and deletion of environments
    - Change Management
    - Maintenance
    - Monitoring Management
    - Capacity Management
    - Infrastructure Support
    - Backup Management
    - Vulnerability Management
    - Service Continuity Management

The guidelines are communicated to both internal and external parties, as well as to users.

The organization is certified in accordance with the ISO/IEC 27001 international standard for information security management, ensuring proper information security practices. The certification is audited annually by an independent certification body. Additionally, as required by ISO/IEC 27001, an internal audit of the ISMS and information security controls is conducted, with the organization engaging a specialized auditor with the necessary credentials.

❖ Data

The organization has operational processes for safeguarding and recovering information that is critical to the provision of services. The information is protected through network segregation and logical access control.

Access to customer environments is done through secure connections (VPN tunnel).

All data access goes through an approval and profile validation process.

The organization does not operate with the client's information. Its function is to protect and conserve it throughout its life cycle.

Tools are in place for validating and monitoring integrity and availability, while confidentiality is safeguarded at all times through stringent access control systems (Google IAM Service) and data encryption (SSL tunnels, database encryption, and server encryption).

7. SECTION II - Security, Availability and Confidentiality Trust Service Principles, Applicable Criteria and Related Controls

This report aims to provide stakeholders with an understanding of the security controls implemented by BOTMAKER to mitigate relevant risks to user organizations. The approach used to examine the design of BOTMAKER's controls was limited to the Trust Services Principles of Security, Availability, and Confidentiality (TSP), along with the related criteria and controls specified by BOTMAKER's senior management.

Common criteria for all principles of security, availability, processing integrity and confidentiality				
CC1.0	**Common criteria related to organization and management**	**Organizational Controls**	***Tests conducted***	***Tests results***
CC1.1	The entity has established organizational structures, reporting lines, authorities and responsibilities for the design, development, implementation, operation, monitoring and maintenance of the system, which allows it to comply with its commitments and requirements related to security, availability, integrity and confidentiality.	Ctrl-1) The organization's work team signs a confidentiality agreement and Code of Conduct. Additionally, confidentiality agreements are signed with critical suppliers. Ctrl-2) The reporting line is clearly defined and communicated to all personnel. There is an organizational chart and a document describing job profiles: the main functions and responsibilities, as well as the knowledge and skills required for each position. The organization's management is notified of each incident or relevant security risk identified.	Ctrl-1) The existence of Confidentiality Agreements and Code of Conduct was verified. Ctrl-1) Existence of Non-Disclosure Agreements and Code of Conduct Verified The following documentation and associated records were verified: - Confidentiality and Intellectual Property Employees V2.0 - DG-01 Code of Conduct V1.0, dated 11/08/2021 - Signed Non-Disclosure Agreement from the Board of Directors, dated 10/28/2024 Ctrl-2) The following documentation and associated records were verified: - BOTMAKER Organization Chart V3.0 date 05/05/2023). It defines the role of "Information Security Analyst", in charge of security design and administration. - The activities related to monitoring, maintenance and control of the infrastructure are in charge of the	No exceptions found

			"Infrastructure Team", defined in the organization chart. - Both depend on the Infrastructure Management, responsible for the management of Information Security, and report directly to the Management of the organization, as the highest responsible.	
CC1.2	Responsibility for designing, developing, implementing, operating, monitoring, maintaining and approving the entity's system controls is assigned to individuals within the entity with authority to ensure that policies and other system requirements are effectively promulgated.	Ctrl-1) Roles and responsibilities are defined and communicated to personnel. Ctrl-2) An Information Security Analyst and an Infrastructure Team are defined, which report to Infrastructure Management and are in charge of monitoring technological services and their risks. Ctrl-3) There is a risk management methodology from which the controls to be implemented are derived. Ctrl-4) There is a technological change management procedure that defines the methodology for analyzing, approving and implementing changes in critical platforms. Ctrl-5) Training on information security is provided to employees where information security policies are communicated.	Ctrl-1) The job profile description and internal communication processes were validated. The following documentation and associated records were verified: - PS-05 Human Capital Management Process – V2.1, 08/28/2023, Item 5.7 “Internal Communication” - Roles and Responsibilities V2.0 – 08/29/2023, Job Profiles Ctrl-2) The following documentation and associated records were verified: - BOTMAKER Organizational Chart V3.0 date 05/05/2023). - It defines the role of "Information Security Analyst", in charge of security design and administration. - The activities related to monitoring, maintenance and control of the infrastructure are in charge of the "Infrastructure Team", defined in the organization chart. - Both depend on the Infrastructure Management, responsible for Information Security management, and report directly to the organization's Management, as the highest responsible.	No exceptions found

			Ctrl-3) The Information Security Analyst executes the risk monitoring and records in the matrix - RG-01 Risk Dashboard V1.0 - The procedure adheres to the methodology outlined in: - PS-01 Risk Management Procedure - V1.1, 09/08/2023 - A sample of the risks identified as high-level was selected: o Unavailability of information due to Ransomware attack (ID ER-02). o Cover the SISO position / Hire a SISO (ER-22) o Old API tokens remain active, allowing an attacker to use them (ER-21) Verified that mitigation and continuity strategies were addressed. Ctrl-4) Evidence of a documented Infrastructure Change Management procedure is available: - PS-10 Customer Environment Management V1.2 Item 5.2 Change Management, which is applied by the infrastructure team. - The registration of changes was verified in o RG-07 Vulnerability Tracking and Control Record_Incidents_Changes_V 1.0. o Evidence of Change Log : Whatsapp Update 2.55.1, dated 04/09/2024, Medium Criticality, Status: Done.	

			Ctrl-5) The execution of onboarding courses for new employees is verified, where awareness of Information Security is raised and security policies are communicated. The following sample was verified PPT "Awareness Workshop". A_15 Training Attendance Record Awareness email “How to avoid phishing”, 12/27/2024.	
CC1.3	Personnel responsible for designing, developing, implementing, operating, monitoring and maintaining the system affecting security, availability, integrity and confidentiality have the qualifications and resources to fulfill their responsibilities.	Ctrl-1) The organization has a team specialized in the selection and management of human resources. Ctrl-2) The personnel involved in infrastructure and security services and support are qualified according to their job position. Skills are evaluated by project leaders on an ongoing basis. Ctrl-3) There is a job description document that identifies the roles and responsibilities of personnel.	Ctrl-1) The process of personnel selection and evaluation is assessed: PS-05 Human Capital Management Process - V2.1, 08/28/2023. Ctrl-2) It is verified that project leaders conduct monitoring and evaluation of employees' skills both prior to and during employment, in accordance with point 5.8 'Personnel Evaluation' of the PS-05 procedure. Ctrl-3) The definition of the job profile was validated. The following documentation and associated records were verified: Roles and Responsibilities - Access Record / Roles and Responsibilities - Access Record V2.0, 08/29/2023. Sample: definition of the "Security Analyst" position.	No exceptions found.
CC1.4	The organization has established standards of conduct for employees, implemented screening procedures for candidates and carries out compliance procedures to enable it to meet its commitments and requirements related to security, availability, integrity and confidentiality.	Ctrl-1) The organization's work team signs a confidentiality agreement and an acceptable use policy for assets and systems. Ctrl-2) The organization has internal personnel selection procedures.	Ctrl-1) The existence of Confidentiality Agreements and Code of Conduct was verified. The following documentation and associated records were validated: - Confidentiality and Intellectual Property Employees V1.3. - A-16 Code of Conduct V1.0 dated 11/08/2021.	No exceptions found.

		Ctrl-3) There is a document with the rules of coexistence, including the Information Security policy, which is known and signed by all employees. Ctrl-4) There are disciplinary sanction practices for non-compliance or violations of the information security policies in force.	Ctrl-2) The existence of a personnel selection and evaluation process was verified: - PS-05 Human Capital Management Process - V2.1, 08/28/2023. Ctrl-3) The availability of the document titled “A-16 Code of Conduct” V1.0, dated 11/08/2021, was verified. Ctrl-4) The existence of a disciplinary process was verified. - PS-05 Human Capital Management Process - Section 5.5 Disciplinary Process	

CC2.0	Common Criteria related to communications	Organizational Controls	*Tests conducted*	*Tests results*
CC2.1	Information on the design and operation of the system and its limits has been prepared and communicated to authorized internal and external users so that they can understand their role in the system and the results of the system's operation.	Ctrl-1) Internal Infrastructure Management: the organization has an Environment Management process, which contains the rules and limits related to the deployment, changes, operation, monitoring, maintenance and support of the service infrastructure. Ctrl-2) The organization has a network diagram reflecting the design of the deployed technological architecture. Ctrl-3) Users and accesses are managed and granted by duly documented profiles. Ctrl-4) The client accesses its environment and manages its own users with the minimum security rules defined by the organization, accepting the terms and conditions of use.	Ctrl-1) The availability of an Environment Management process was verified. PS-10 Environment Management. It was validated that it reflects all the main management of the infrastructure operation. V1.2, 01/10/2022 Ctrl-2) The infrastructure design "Network Diagram" - v1.0 was verified. Ctrl-3) Verified the registry Roles and Responsibilities - Access Record / Roles and Responsibilities - Access Record V2.0, 08/29/2023 Ctrl-4) The automatic creation of accounts for system clients/users was verified. Additionally, the existence of a privacy policy, which was validated and accepted by the client, was confirmed: Privacy Policy - Botmaker.com/en/privacy User authentication via their Google or Facebook account, or user creation linked to an email through the Google service, was verified	No exceptions found.
CC2.2	The organization's security, availability, integrity and confidentiality commitments are communicated to external users, as appropriate; these commitments and the associated system requirements are informed to the internal users of the system so that they can fulfill their responsibilities.	Ctrl-1) Security commitments are communicated to clients through specific contracts ("major clients") and the Privacy Policy. Ctrl-2) Employment agreements incorporate provisions and/or terms for compliance with established information security and governance policies and	Ctrl-1) The existence of a privacy policy was validated and accepted by the client: Privacy Policy - Botmaker.com/en/privacy Ctrl-2) Ctrl-3) Validated the existence of Confidentiality Agreements and Code of Conduct. The following documentation and associated records were verified:	No exceptions found.

		must be reviewed and accepted by staff. Ctrl-3) There are confidentiality agreements and coexistence rules, including the Information Security policy, which is known and signed by all employees.	- Confidentiality and Intellectual Property Employees V1.3 - A-16 Code of Conduct V1.0 dated 11/08/2021.	
CC2.3	The entity communicates responsibilities to internal and external users and any other role that affects the operation of the system.	Ctrl-1) Formal specification of job profiles. Ctrl-2) Existence of confidentiality agreements and codes of conduct. Ctrl-3) Agreement on privacy and use of systems.	Ctrl-1) The record was verified. Roles and Responsibilities - Access Record / Roles and Responsibilities - Access Record V2.0, 08/29/2023. Ctrl-2) The following documentation and associated records were verified: Confidentiality and Intellectual Property Employees V2.0. A-16 Code of Conduct V1.0 dated 11/08/2021. Ctrl-3) Validated the existence of a privacy policy which the client accepts: Privacy Policy - Botmaker.com/en/privacy	No exceptions found.
CC2.4	Internal and external personnel responsible for designing, developing, implementing, operating, monitoring and maintaining the system's controls, relevant to security, availability, processing, integrity and confidentiality, have the necessary information to carry out these responsibilities.	Ctrl-1) Existence of an Environment Management Procedure that includes the Deployment, disposal, maintenance, operation, monitoring, support and maintenance of productive environments and systems.	Ctrl-1) The existence of an Environment Management process was verified. - PS-10 Environment Management 1.2	No exceptions found.
CC2.5	Internal and external users of the system receive information on how to report security, availability, integrity and confidentiality failures, incidents, concerns and other complaints to the appropriate personnel.	Ctrl-1) Formal channels are defined for reporting failures and security incidents. A documented Information Security Incident Management procedure is in place.	Ctrl-1) The existence of a security incident management process was verified: - PS-11 Incident Management - V1.0 - 12/06/2021. Ctrl-2) The communication channels available to the client were validated: - Account manager	No exceptions found.

		Ctrl-2) Formal communication channels are in place with the client for reporting information security failures.	- Partners - Mail The communication of a formal channel for reporting issues related to the processing of personal data was validated: - Privacy Policy - Botmaker.com/privacy	
CC2.6	Changes to the system that affect the internal and external responsibilities of system users or the entity's commitments and requirements related to security, availability, integrity and confidentiality are communicated to the users in a timely manner.	Ctrl-1) All changes that may affect the operation and security of the systems are communicated and coordinated with the interested parties. There is an Infrastructure Change Management procedure.	Ctrl-1) The existence of a change management process was verified: - PS-10 Environment Management - Section 5.2 Change Management. It was verified that changes are recorded in - RG-07 Vulnerability Monitoring and Control Record_Incidents_Changes. - Sample: Whatsapp software update 2.55.1, 04/09/2024, result "done".	No exceptions found.

CC3.0	Common Criteria related to Risk Management, control design and implementation	Organizational Controls	Tests conducted	Tests results
CC3.1	The organization (1) identifies potential threats that could affect system security, availability, integrity and confidentiality commitments and requirements, (2) analyzes the significance of the risks associated with the identified threats, and (3) determines mitigation strategies for these risks (including controls and other mitigation strategies).	Ctrl-1) Periodically, the technology management, with the support of the Security Analyst, performs an analysis of existing risks for various high-impact risk scenarios. Ctrl-2) Business continuity plans are defined to respond to the continuity of customer services in the event of an interruption of operations as a risk mitigation strategy. Ctrl-3) Risks are reviewed periodically and their treatment is monitored.	Ctrl-1) The existence of a Risk Management process is verified. - PS-01 Risk Management Procedure - V1.1, 09/08/2023. The technological risk management matrix (RG-01 Risk Dashboard) was reviewed. Evidence of the status of risk treatment and its follow-up is available. - Risk ID ER-09 Unauthorized access due to inadequate network architecture design or segregation. Treatment Trello ID tFKNly1e. Status Closed. Ctrl-2) Contingency strategy and continuity test execution were validated. - Contingency Strategy.xlsx, Date 07/10/2023. - Test Exercise on the scenario “Unavailability due to critical DB failure” – 04/04/2024. Ctrl-3) The definition of risk review was verified on an annual basis (Risk Monitoring - PS01).	No exceptions found.
CC3.2	The organization designs, develops and implements controls, including policies and procedures, to implement the risk mitigation strategy.	Ctrl-1) The organization has implemented an ISMS - Information Security Management System, based on and certified under the ISO/IEC 27001 Information Security Management Standard. Ctrl-2) Policies and procedures for information security management are in place.	Ctrl-1) The documented ISMS, certified under ISO/IEC 27001 is verified. Ctrl-2) The availability of documented policies and procedures that respond to a risk mitigation strategy is verified: - Statement of Applicability (DDA) v1.1, 09/08/2023.	No exceptions found.

		Ctrl-3) Availability of an Objectives and Management V1.1 dashboard to monitor operational controls, security and management indicators.	Ctrl-3) The definition and monitoring of controls associated with the ISMS as a risk mitigation strategy was validated: - RG06-Objectives And Management Dashboard v2.0 01/03/2023.	
CC3.3	The organization (1) identifies and evaluates changes (e.g., environmental, regulatory, and technological changes) that could significantly impact the internal control system for security, availability, processing integrity, and confidentiality and reassesses the risks and mitigation based on the changes and (2) reassesses the adequacy of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.	Ctrl-1) Availability of the ISMS context and scope definition and analysis document. Ctrl-2) Context and strategic objectives reviews are carried out annually by the Management, resulting in a SWOT/DAFO Matrix. Ctrl-3) There is a formal documented procedure for Infrastructure Change Management. Ctrl-4) Existence of a process for document management, including the management of documentary changes (updates to policies, processes, procedures, etc.).	Ctrl-1) The availability of the document was verified. - Context and Scope of the ISMS - V2.1 09/08/2023 Ctrl-2) Validated the SWOT matrix and the annual management review: - DG-02 SWOT-CAME Matrix - V1.1 - 11/08/2022 08/11/2022. Last Revision performed on 11/19/2024. - PS-04 Management Review - V1.0 - 09/28/2021. The management review was validated, including the treatment of the context change review, SWOT and Risk management: - A-03 Minutes of Management Review dated 03/04/2024. Ctrl-4) The existence of the documented information management procedure was verified: - PR-01 Documented Information Management Procedure - V2.1 - 09/08/2023	No exceptions found.

CC4.0	Common Criteria related to Controls Monitoring	Organizational Controls	Tests conducted	Tests results
CC4.1	The design and operating effectiveness of controls are periodically evaluated for security and availability.	Ctrl-1) Availability and security operational monitoring tools and controls in place. Ctrl-2) Availability indicators associated with system availability and security incidents and infrastructure support. Ctrl-3) Annual review of ISMS Ctrl-4) Annual audits of the ISMS Ctrl-5) VRA/Pentest type audits on infrastructure Ctrl-6) Monitoring and Management of Vulnerabilities in the systems. Ctrl-7) Non-conformity management and continuous improvement process.	Ctrl-1) The availability of a monitoring management process was verified: - PS-10 Environment Management - Section 5.4 Monitoring Management - PS-10 Environment Management - Section 5.6 Infrastructure Support The following record was validated: - RG-07 Vulnerability Monitoring and Control Log_Incidents_Changes". - Uptime Checks.xls o 04/30/2024 result: 99.9970% o 05/31/2024 result: 99.9810% Ctrl-2) The following record was validated: - RG06 - Objectives and Management Dashboard v2.0 01/03/2023 - Sample: Control "Security Incidents with Deviations in Response Time as of 09/15/2023," indicator in "green" status. - Sample: Security Incidents 05/29/2024 Ctrl-3) Management review was validated, including updates and changes to the ISMS. - A-03 Management Review Minutes dated 03/04/2024. Ctrl-4) The execution of the last internal and external audit of the ISMS was confirmed. - Internal Audit Report - Information Security Management, dated 01/20/2025. - Audit Findings Review Report. - Follow-up Audit Report - Issued by IRAM - dated 03/06/2024.	No exceptions found.

			Ctrl-5) The execution of an annual pentest was verified: - BotMaker - Technical Report Re-Test - Web GreyBox Pentest - 01/24/2025. Ctrl-6) The record was validated: - “RG-07 Tracking and Control Register for Vulnerabilities, Incidents, and Changes”. Sample: Resolved vulnerabilities from the retest – “Request Forgery (localhost bypass),” 01/23/2025. Ctrl-7) The existence of the non-conformities and improvement management procedure was verified. - PS-02 Continuous Improvement Process V1.0 - 09/13/2021 - RG-02 Continuous Improvement Follow-Up Record - updated to date	

CC5.0	Common Criteria related to Physical and Logical Access Controls	Organizational Controls	Tests conducted	Tests results
CC5.1	Logical access security software, infrastructure and architectures have been implemented to support: (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output and offline items; and (3) prevention and detection of unauthorized access.	Ctrl-1) There are documented procedures for access management. Ctrl-2) The organization has a Password Policy. Ctrl-3) All authentication systems associated with the infrastructure and systems allow the creation of strong passwords and compliance with defined password policies. Ctrl-4) The authentication systems have controls for blocking passwords due to repeated incorrect entries and alerts the administrator.	Ctrl-1) The existence of the access management procedure was verified, which is adequate for the organization. - PS-07 Access Management, v1.3, 09/15/2023 Ctrl-2) The existence of a password policy was verified, which is adequate for the organization. - POL-02 Particular Information Security Policies - v1.3, dated 05/04/2023 - Paragraph 2.8 Password Policy. Ctrl-3) Verified the "Google" Authentication configured according to the policies for the environments and infrastructure systems. Verified the use of Google IAM for access to critical infrastructure. For critical systems, the existence of two-factor authentication was validated. For the user environment, authentication is by means of a personal Google or Facebook account, or by creating a user associated with an email through the Google service. Ctrl-4) The system's ability to generate email alerts for administrators in response to unauthorized access attempts was validated.	No exceptions found.
CC5.2	New users, whether internal or external to the system, are registered and authorized before receiving system credentials and being granted the ability to access the system. The user's system credentials are removed when the user's access is no longer authorized.	Ctrl-1) System access is authorized for new users before they are granted the ability to access the organization's systems.	Ctrl-1) The network user approval and granting circuit has been validated for a new user registration. - Example: User registration May/09/2022 reported in Google Workspace.	No exceptions found.

		Ctrl-2) Role-based access is used to determine the need for access to systems. Ctrl-3) Users and permissions are removed according to the Access Management document procedure. Ctrl-4) There are regular controls for access and removal of granted accesses..	Ctrl-2) Access rights were validated according to the user profile associated with the 'Security Analyst' role, confirming compliance with the definitions outlined in the record: - Roles and Responsibilities – Access Profile v2.0, 08/29/2023. Ctrl-3) The deletion of users after their cancellation was validated according to PS-07 Access Management, Version 1.3, 09/15/2023. - Section 5.3 Termination of users. Ctrl-4) he execution of the semi-annual access review was validated. - RG06 - Objectives and Management Dashboard v2.0, 01/03/2023 - Privileged users – Last review date: 01/10/2025 – No deviations - Standard users – Last review date: 01/10/2025 – No deviations - The scheduling of a review for deactivated users on 07/30/2025 was validated.	
CC5.3	Internal and external system users are identified and authenticated when accessing system components (e.g., infrastructure, software, and data).	Ctrl-1) All system components have secure logical access authentication systems.	Ctrl-1) Reviewed relevant service access systems: ● Google Cloud ● Databases ● GitHub (access to source code) ● Botmaker platform administration ● Access as a client of the Botmaker platform All accesses required a username and password duly granted according to the profile to access it.	No exceptions found.
CC5.4	Access to data, software, functions and other IT resources is authorized and modified or removed based on roles, responsibilities, or system design and	Ctrl-1) Role-based access is used to determine the need for access to systems.	Ctrl-1 and Ctrl-2) It was verified that procedures exist for granting, modifying, and deleting access to data, software, and other resources, all based on user roles.	No exceptions found.

	changes to them.	Ctrl-2) Access to the network and systems is revoked or modified as part of the access management process. Ctrl-3) For Botmaker platform users (clients), the system allows user creation, modification and deletion.	- PS-07 Access Management, Version 1.3, 09/15/2023 Ctrl-3) Access as a client to the Botmaker platform, creation, modification and deletion of users was validated.	
CC5.5	Physical access to the facilities hosting the system (e.g., data centers, backup media storage and other confidential locations, as well as sensitive system components within those locations) is restricted to authorized personnel.	Ctrl-1) The organization has all of its infrastructure in the Google cloud. Therefore, everything related to physical access is being covered. Ctrl-2) The applications and internal management support systems are contracted as a cloud service (SaaS).	Ctrl-1) It was validated that all infrastructure directly or indirectly associated with customer service is deployed in the Google cloud. Ctrl-2) It was validated that all support and internal management services are deployed in GCP or are SaaS type services contracted to first level companies (GitHub, YouTrack, among others).	No exceptions found. .
CC5.6	Logical access security measures have been implemented to protect against unauthorized access and threats to availability, integrity and confidentiality from sources outside the system boundaries.	Ctrl-1) Access to the infrastructure is done through IAM - Identity and Access Management of Google Cloud. Ctrl-2) Accesses with critical privileges are controlled every 15 days and every 6 months for non-critical ones. Ctrl-3) Accesses of users accessing the infrastructure are controlled through a Firewall and the corresponding enabling of origin and ports.	Ctrl-1) Access management was validated through IAM. Ctrl-2) Periodic control of privileged accesses was verified: - Critical. Last record dated 01/10/2025. - Non-critical. Last record dated 01/10/2025. Ctrl-3) The documented access registered in [Botmaker] Firewall Access.xls was validated vs. the firewall.	No exceptions found.
CC5.7	The transmission, movement and disposal of information is restricted to authorized users and processes, and is protected during transmission, movement or disposal, enabling the entity to meet its commitments and requirements regarding security, availability, integrity and confidentiality.	Ctrl-1) Existence of a policy for the exchange and treatment of client information. Ctrl-2) The information managed by the client through the platform is managed by the client throughout its life cycle; the organization only intervenes in the backup.	Ctrl-1) The existence of the policy was verified: - POL-02 Specific information security policies - v1.3, dated 05/04/2023 - Section 2.4 Customer information exchange and processing policy. Ctrl-2) The existence of access profiles for users and their permissions to manage their information through the platform was validated.	No exceptions found.

		Ctrl-3) There is a strict control over the granting and execution of permissions for the transmission, movement and elimination of data from the systems. Ctrl-4) Every change, whether it is the deletion or movement of a database, goes through a clearly defined Change Management process.	Ctrl-3) Verified the existence of procedures for granting role-based access to data, as well as its modification and elimination. - PS-07 Access Management, Version 1.3, 09/15/2023 Ctrl-4) The existence of a change management process was verified: - PS-10 Environment Management - Section 5.2 Change Management. It was verified that the changes are recorded in: - "RG-07 Vulnerability Tracking and Control Record_Incidents_Changes". Sample: Whatsapp software update 2.55.1, 04/09/2024, result: "done".	
CC5.8	Controls are in place to prevent or detect and act upon the introduction of unauthorized or malicious software.	Ctrl-1) Existence of a policy for the acquisition of software. Ctrl-2) Existence of a policy for the proper use of information systems. Ctrl-3) At the infrastructure level, all software must be homologated and go through a change management process..	Ctrl-1) Verified the existence of the policy: - POL-02 Particular Information Security Policies - v1.3, dated 05/04/2023 - Section 2.9 Software Acquisition and Systems Interconnection Policy. Ctrl-2) Verified the existence of the policy: - POL-02 Specific Information Security Policies - v1.3, dated 05/04/2023 - Section 2.9 Software Acquisition and Systems Interconnection Policy. Ctrl-3) Verified the availability of a change management process: - PS-10 Environment Management - Section 5.2 Change Management.	No exceptions found.

CC6.0	Common Criteria related to Operating Systems	Organizational Controls	Tests conducted	Tests results
CC6.1	Vulnerabilities of system components to security, availability, integrity, confidentiality breaches and incidents due to malicious acts, natural disasters or errors are monitored and evaluated, and countermeasures are implemented to compensate for new and known vulnerabilities.	Ctrl-1) The organization has a vulnerability management process. Ctrl-2) Annual vulnerability scans and Penetration Tests are performed. Ctrl-3) Systems are monitored and analyzed for vulnerabilities. Ctrl-4) Vulnerabilities are managed and prioritized according to their criticality.	Ctrl-1) The existence of a monitoring management process was verified: - PS-10 Environment Management - Section 5.8 Vulnerability Management. Ctrl-2) The completion of the annual Penetration Test was verified: - BotMaker - Technical Re-Test Report - Web GreyBox Pentest - 01/24/2025. Ctrl-3 and Ctrl-4) The register was validated: - "RG-07 Vulnerability Monitoring and Control Register _Incidents_Changes" The management of the following vulnerabilities, selected by sampling, was verified: - CVE-2023-33064 on the orche-chore component – detection 10/05/2024. - CVE-2023-9113 on the orche-chore component – detection 10/05/2024.	No exceptions found.
CC6.2	Security, availability, integrity and confidentiality incidents, including breaches, failures, concerns and other logical and physical security complaints, are identified, reported to appropriate personnel and acted upon in accordance with established incident response procedures.	Ctrl-1) There is a formal documented security incident management procedure. Ctrl-2) Formal channels for reporting failures and security incidents are defined. Ctrl-3) Incidents are analyzed and managed according to defined processes.	Ctrl-1) The existence of a security incident management process was verified: - PS-11 Incident Management - V1.0 - 12/06/2021. Ctrl-2) The communication channels available to the client were validated: ➔ Account manager ➔ Partners ➔ Mail Validated the communication of a formal channel to report issues related to the processing of personal data: - Privacy Policy - Botmaker.com/privacy Ctr-3) The following record was validated "RG-07 Vulnerability Monitoring and Control Record _Incidents_Changes".	No exceptions found.

			The management of the following incidents, selected by sampling, was verified: - Incident related to Console transaction processing services – 10/07/2024. Platform functionality interruptions. - Incident related to Webchat – 07/31/2024. Webchat issues. Both incidents were managed and resolved without deviations.	

CC7.0	*Common Criteria related to Change Management*	Organizational Controls	*Tests conducted*	*Tests results*
CC7.1	Security, availability, integrity and confidentiality requirements and commitments are addressed throughout the system development life cycle, including design, acquisition, implementation, configuration, testing, modification and maintenance of system components.	Ctrl-1) The personnel assigned to the service act in accordance with the organization's guidelines and those defined by the client with respect to security, integrity, availability and confidentiality, throughout the software development life cycle. Ctrl-2) Changes and maintenance in operation are managed through an environment management process.	Ctrl-1) It is verified that the organization follows methodologies and good practices in software development. Ctrl-2) The existence of a change and maintenance management process was verified: - PS-10 Environment Management - Section 5.2 Change Management. - PS-10 Environment Management - Section 5.3 Maintenance	No exceptions found..
CC7.2	Infrastructure, data, software and procedures are updated as necessary to maintain consistency with system commitments and requirements for security, availability, integrity and confidentiality of processing.	Ctrl-1) A component maintenance plan is defined using metrics and alerts, in order to update the components. Google Cloud actions are configured to automatically update components according to the criticality of the change. Ctrl-2) Google Cloud alerts regarding component update status are monitored and acted upon according to the Change Management process. Ctrl-3) Procedures are updated upon changes. An annual review of all procedures is performed.	Ctrl-1 and Ctrl-2) The configuration of metrics in the different components of the systems and the reception of alerts were validated. Ctrl-3) The Documented Information Management Procedure was verified: - PR-01 Documented Information Management Procedure - V2.1.0 - 09/08/2023. It was confirmed that all documents have a current version, with no publication or modification dates older than 12 months.	No exceptions found.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Ctrl-1) The Change Management process is executed when a modification or problem/incident resolution is required.	Ctrl-1) The existence of a change management process was verified, which defines the guidelines for requesting, evaluating and executing changes. - PS-10 Environment Management - Section 5.2 Change Management	No exceptions found.

CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved and implemented in accordance with security, availability, processing integrity and confidentiality commitments and requirements.	Ctrl-1) Changes are categorized according to their criticality, from which planning, approval and registration requirements are defined.	Ctrl-1) The following steps in the definition and execution of changes were verified based on their criticality, categorized as follows: - **Standard**: routine changes without risk to the operation. For example, application of non-critical patches. - **Critical**: require, due to their complexity or potential impact, a detailed planning, analysis and formal approval. For example, migration of a database. - **Emergent**: result from the need for immediate execution. For example, to resolve an incident.	No exceptions found.

Additional Criteria for Availability		Organizational Controls	*Tests conducted*	*Tests results*
A1.1	Current processing capacity and usage are monitored, maintained and evaluated to manage capacity demand and enable the implementation of additional capacity to help meet commitments and availability requirements.	Ctrl-1) The capacity of critical components is monitored through metrics and alarms. Ctrl-2) All infrastructure used is self-scalable as part of the solutions provided by the cloud service provider.	Ctrl-1) Alerts were validated for: - Capacity of the "queues" - "Infrastructure queues alert" log. - CPU and Memory monitoring graphs- Sample: cpu near limit on m-infra. Ctrl-2) It was validated that all services run on Google Cloud with a service that allows infrastructure auto scaling. In the case of receiving CPU alerts due to saturation, its capacity is expanded.	No exceptions found.
A1.2	Environmental protections, software, data backup processes and recovery infrastructure are designed, developed, implemented, operated, monitored and maintained to meet availability commitments and requirements.	Ctrl-1) A backup management process is in place. Ctrl-2) There is a Contingency Management process. Ctrl-3) The environmental conditions of the infrastructure are ensured by the cloud infrastructure provider.	Ctrl-1) The existence of a safeguards management process was verified. - PS-10 Environment Management - Section 5.7 Safeguards Management Ctrl-2) The existence of a safeguards management process was verified. - PS-10 Environment Management - Section 5.9 Continuity of Service Ctrl-3) Validated the supplier's compliance with SOC 2: https://cloud.google.com/security/compliance/soc-2.	No exceptions found.
A1.3	Procedures that support system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	Ctrl-1) Documented backup strategies and execution of periodic tests. Ctrl-2) Documented strategies for Service Contingency Management and periodic testing..	Ctrl-1) The backup strategy and the execution of restore tests were validated: - Vulnerability Tracking and Control Log_Incidents_Changes - V1 - "Backup Policy and Execution". Ctrl-2) The contingency strategy and the execution of continuity tests were validated. - Contingency Strategy.xlsx,dated 07/10/2023.	No exceptions found.

			- Test Exercise on the scenario 'Unavailability due to critical DB failure' – 04/04/2024.	

Additional Criteria for Availability		Organizational Controls	*Tests conducted*	*Tests results*
PI1.1	Procedures are in place to prevent, detect and correct processing errors to comply with processing integrity commitments and requirements.	Ctrl-1) The platform has data integrity controls in place. Ctrl-2) There is an incident management procedure available to handle any processing and/or data integrity errors.	Ctrl-1) Validation of the existence of input data validation controls and information exchange through APIs. Ctrl-2) The existence of a security incident management process was verified: - PS-11 Incident Management - V1.0 - 12/06/2021	No exceptions found.
PI1.2	System inputs are measured and recorded in a complete, accurate and timely manner in accordance with processing integrity commitments and requirements.	Ctrl-1) There is an integrity check on data inputs to the platform. Ctrl-2) Relevant entries and activities are recorded in the platform transaction log.	Ctrl-1) The existence of customizable input data validation controls within the platform configuration was verified: - Configuration of question "User name", valid input data set to type "Name". Ctrl-2) The following entries in the change history log were validated through sampling: - Date - Identifier - Priority - Slot	No exceptions found.
PI1.3	Data is processed in a complete, accurate and timely manner as authorized, in accordance with processing integrity commitments and requirements.	Ctrl-1) Data not complete or with any integrity validation error are not processed.	Ctrl-1) The following inputs, their validation before processing and the error message to the user were checked by sampling: - Question configuration "User name", valid input data type "Name".	No exceptions found.

PI1.4	Data is stored and maintained completely and accurately for its specified lifetime in accordance with processing integrity commitments and requirements.	Ctrl-1) Data is stored and maintained in full compliance with the specifications defined in the contractual Terms and Conditions. Ctrl-2) The defined backup strategy meets the backup requirements.	Ctrl1) The following statement in the Privacy Policy was validated https://Botmaker.com/es/privacy/ "Term: Botmaker may retain Information for as long as necessary to fulfill the purposes for which it was collected or as necessary to provide the Services, including after it has discontinued or deleted any account, or after the termination of the provision of the Services, if the retention of such Information is reasonably necessary to comply with legal obligations, comply with regulatory requirements, resolve disputes between users, prevent fraud, or any other use." Ctrl-2) The backup scheme defined for the following databases was validated: ● Firestore - Full ● BigQuery - Incremental ● Kubernetes objects - Full /Backup Type: Full / Incremental /Periodicity: Daily /History: not limited	No exceptions found.
PI1.5	System output is complete, accurate, distributed and retained in accordance with processing integrity commitments and requirements.	Ctrl-1) There is an integrity control over the platform's data outputs. Ctrl-2) Relevant outputs and activities are recorded in the platform transaction log.	Ctrl-1) Existence of output data validation controls was validated. - In case of an invalid name entry in the "name type" field, an error output message is returned. Ctrl-2) The following outputs in the platform's conversation event log were validated by sampling: - Sending undelivered notifications by Whatsapp channel.	No exceptions found.

PI1.6	Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Ctrl-1) Platform users can only modify the information associated with their profile. Ctrl-2) Any modification of information outside the logic of the platform operation, goes through a process of analysis and authorization (Change Management).	Ctrl-1) The operations that can be executed by a user of the platform were validated and were in accordance with the assigned profile. Ctrl-2) The existence of a change management process was verified, which defines the guidelines for requesting, evaluating and executing changes. - PS-10 Environment Management - Section 5.2 Change Management	No exceptions found.

Additional Criteria for Availability		Organizational Controls	*Tests conducted*	*Tests results*
C1.1	Confidential information is protected during the system design, development, testing, implementation and change processes in accordance with confidentiality commitments and requirements.	Ctrl-1) No production data is used in any previous environment. Ctrl-2) All production changes go through a controlled process (Change Management).	Ctrl-1) The development team was interviewed, and it was confirmed that production data is not used for debugging or testing. Ctrl-2) The existence of a change management process was verified, which defines the guidelines for requesting, evaluating and executing changes. - PS-10 Environment Management - Section 5.2 Change Management	No exceptions found.
C1.2	Confidential information within system boundaries is protected from unauthorized access, use and disclosure during input, processing, retention, output and disposition in accordance with confidentiality commitments and requirements.	Ctrl-1) Users must authenticate their access to the client environment through a username and password. Ctrl-2) User access to the platform environment as support or assistance has an approval and monitoring flow. Ctrl-3) There are cryptographic controls for the transmission, processing and safeguarding of sensitive information..	Ctrl-1) Verified the authentication of users through their "Google" or "Facebook" account or the creation of a user associated with an email through the Google service. Ctrl-2) The existence of a semi-automatic access request process for platform access by user support operators, when needed, was verified. Permission is granted for a maximum of 24 hours and revoked once the assistance is completed. All activities performed are logged and managed through the https://iaccess.Botmaker.app module. Ctrl-3) It is verified that you the following control is in place: - SSL channel on the complete platform	No exceptions found.
C1.3	Access to confidential information from outside the system boundaries and disclosure of confidential information is restricted to authorized parties in accordance with confidentiality commitments and requirements.	Ctrl-1) Access to the infrastructure by privileged users is restricted to authorized personnel according to their job profile.	Ctrl-1) The access rights defined in the "Roles and Responsibilities - Access Profile" record are validated by sampling: # "Google Cloud Customer Environment". - Management Type: by Owner	No exceptions found.

		Ctrl-2) There are cryptographic controls in the infrastructure for accessing and safeguarding information.	- Owner: Director of Engineering and Infrastructure Manager - Access: Owner only # GitHub - Management type: by profile - Owner: Infrastructure Manager - Access: technology roles. Ctrl-2) It is verified that the following controls are applied: - VPN for access to platform infrastructure management. - AES256 encryption on servers.	
C1.4	The organization obtains confidentiality commitments that are consistent with the entity's confidentiality requirements from suppliers and other third parties whose products and services are part of the system and have access to confidential information.	Ctrl-1) There are confidentiality commitments with employees that are consistent with the commitment made to the client. Ctrl-2) There are confidentiality commitments with suppliers that are consistent with the commitment made to the client.	Ctrl-1) The following documentation and associated records were verified: - Confidentiality and Intellectual Property Employees V2.0. - A-16 Code of Conduct V1.0 dated 11/08/2021. Ctrl-2) The confidentiality commitment of the main supplier associated with the service was validated: - https://cloud.google.com/privacy Validated, as applicable, the signature of agreements with suppliers. - A-14 Confidentiality agreement with suppliers.	No exceptions found.
C1.5	Compliance with confidentiality commitments and requirements by suppliers and other third parties whose products and services are part of the system is evaluated periodically and as necessary and, if necessary, corrective actions are implemented.	Ctrl-1) Stakeholder requirements associated with confidentiality and legal and contractual compliance are reviewed at least once a year. Ctrl-2) A supplier security assessment is performed once a year.	Ctrl-1) Stakeholder requirements analysis was verified. - DG-03_Stakeholder Requirements - Last review: 12/20/2022. Ctrl-2) RG-01 Supplier Evaluation Record V1.0 10/18/2021. Supplier Analysis Sampling: - Google Cloud: 08/31/2024 - Linkedin: 08/31/2024.	No exceptions found.

C1.6	Changes in confidentiality commitments and requirements are communicated to internal and external users, suppliers and other third parties whose products and services are included in the system.	Ctrl-1) Changes in internal confidentiality agreements with impact are communicated to employees and a new contract is signed. Ctrl-2) Changes in agreements with customers (external users) are communicated through the privacy policy published on the Web.	Ctrl-1) It was confirmed that any changes to the confidentiality agreement are assessed within the Human Capital Management process to determine whether employees need to re-sign it. Currently, there have been no version changes requiring re-validation by employees. Ctrl-2) The publication of the privacy policy https://Botmaker.com/privacy/ was validated.	No exceptions found.

IQNET

Building trust together.

Certificate

IRAM has issued an IQNET recognized certificate that the organization:

BOTMAKER ARGENTINA - BOTMAKER S.R.L. / BOTMAKER USA - BOTMAKER INC / BOTMAKER BRASIL - BM BRASIL INTERNET LTDA.

Casa central: Virrey Olaguer y Feliú 2535 - (C1426EBC) - Ciudad Autónoma de Buenos Aires - República Argentina
Sitio Brasil: R. Pirandello 45 - (04623-000) - São Paulo - República Federativa do Brasil
Sitio EEUU: 3390 Mary St Suite 310 - (33131) - Miami - Florida - Estados Unidos de América

has implemented and maintains a/an

Information security Management System

for the following scope:

Administration, operational support, and maintenance of the infrastructure of the service provided through the Botmaker platform in its software as a service (SaaS) format. Taking into consideration the protection of personal data that may be stored, transmitted, or processed.

which fulfils the requirements of the following standard;

ISO/IEC 27001:2022

Issued on: **31/10/2025**
Expires on: **31/10/2028**

Registration Number: **AR - IS - 148**

Alex Stoichitoiu
President of IQNET

Gustavo Pontoriero
Certification Division Manager

IRAM Instituto Argentino de Normalización y Certificación

This attestation is directly linked to the IQNET Member's original certificate and shall not be used as a stand-alone document.

IQNET Members*:
AENOR Spain **AFNOR Certification** France **APCER** Portugal **CCC** Cyprus **CISQ** Italy **CQC** China **CQM** China **CQS** Czech Republic **Cro Cert** Croatia **DQS Holding GmbH** Germany **EAGLE Certification Group** USA **FCAV** Brazil **FONDONORMA** Venezuela **ICONTEC** Colombia **ICS** Bosnia and Herzegovina **Inspecta Sertifiointi Oy** Finland **INTECO** Costa Rica **IRAM** Argentina **JQA** Japan **KFQ** Korea **LSQA** Uruguay **MIRTEC** Greece **MSZT** Hungary **Nemko AS** Norway **NSAI** Ireland **NYCE-SIGE** México **PCBC** Poland **Quality Austria** Austria **SII** Israel **SIQ** Slovenia **SIRIM QAS International** Malaysia **SQS** Switzerland **SRAC** Romania **TSE** Turkey **YUQS** Serbia

* The list of IQNET Members is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

CERTIFICADO DE SISTEMAS DE GESTIÓN

Miembro de IQNET

IRAM certifica que:

BOTMAKER ARGENTINA - BOTMAKER S.R.L. / BOTMAKER USA - BOTMAKER INC / BOTMAKER BRASIL - BM BRASIL INTERNET LTDA.

Casa central: Virrey Olaguer y Feliú 2535 - (C1426EBC) - Ciudad Autónoma de Buenos Aires - República Argentina
Sitio Brasil: R. Pirandello, 45 - (04623-000) - São Paulo - República Federativa do Brasil
Sitio EEUU: 3390 Mary St Suite 310 - (33131) - Miami - Florida - Estados Unidos de América

posee un **Sistema de Gestión de la Seguridad de la Información** que cumple con los requisitos de la norma:

IRAM - ISO/IEC 27001:2024

Registro N.º 27000-148

Cuyo alcance es:

Administración, soporte operativo y mantenimiento de la infraestructura del servicio brindado a través de la plataforma Botmaker en su modalidad de "Software as a Service" (SaaS). Teniendo en cuenta la protección de los datos personales que pudieran almacenarse, transmitirse o procesarse.

Emisión: 11/11/2025

Vigencia: 31/10/2025 a 31/10/2028

Gustavo Pontoriero
Gerente de División SG&CP
Certificación IRAM
(Firmado digitalmente)

Este certificado es válido siempre que la organización mantenga en operación, en condiciones satisfactorias, su Sistema de Gestión de la Seguridad de la Información y que cumpla con el acuerdo de certificación DC-R 010 y el manual DC-PG 096.

DC-FL 069

Ciudad Autónoma de Buenos Aires, 05 de noviembre de 2025.

Señores de
BOTMAKER ARGENTINA - BOTMAKER S.R.L. / BOTMAKER USA - BOTMAKER INC / BOTMAKER BRASIL - BM BRASIL INTERNET LTDA.
Presente

Asunto: Otorgamiento de la certificación

De nuestra mayor consideración:

En nombre del Instituto Argentino de Normalización y Certificación (IRAM) le hago llegar nuestra felicitación a su organización por obtener la certificación basada en la norma **IRAM-ISO/IEC 27001:2024.** Difundiremos el logro alcanzado en listados de organizaciones certificadas, página web y otras presentaciones que eventualmente realicemos.

IRAM agradece que nos haya elegido como su organismo de certificación, esperando brindarle en cada oportunidad un mejor servicio, recorriendo juntos el camino hacia la mejora continua.

Los saludo atentamente.

hernan@botmaker.com

Gustavo Pontoriero
Gerente División SG&CP
Certificación IRAM

Instituto Argentino de Normalización y Certificación

Ciudad Autónoma de Buenos Aires, 05 de noviembre de 2025.

Señores de

BOTMAKER ARGENTINA - BOTMAKER S.R.L. / BOTMAKER USA - BOTMAKER INC / BOTMAKER BRASIL - BM BRASIL INTERNET LTDA.

Presente

Asunto: Otorgamiento de la certificación

De nuestra mayor consideración:

En nombre del Instituto Argentino de Normalización y Certificación (IRAM) le hago llegar nuestra felicitación a su organización por obtener la certificación basada en la norma **ISO/IEC 27701:2019.** Difundiremos el logro alcanzado en listados de organizaciones certificadas, página web y otras presentaciones que eventualmente realicemos.

IRAM agradece que nos haya elegido como su organismo de certificación, esperando brindarle en cada oportunidad un mejor servicio, recorriendo juntos el camino hacia la mejora continua.

Los saludo atentamente.

hernan@botmaker.com

Gustavo Pontoriero

Gerente División SG&CP

Certificación IRAM

IQNET

Building trust together.

Certificate

IRAM has issued an IQNET recognized certificate that the organization:

BOTMAKER ARGENTINA - BOTMAKER S.R.L. / BOTMAKER USA - BOTMAKER INC / BOTMAKER BRASIL - BM BRASIL INTERNET LTDA.

Casa central: Virrey Olaguer y Feliú 2535 - (C1426EBC) - Ciudad Autónoma de Buenos Aires - República Argentina
Sitio Brasil: R. Pirandello 45 - (04623-000) - São Paulo - República Federativa do Brasil
Sitio EEUU: 3390 Mary St Suite 310 - (33131) - Miami - Florida - Estados Unidos de América

has implemented and maintains a/an

Privacy information management

for the following scope:

Administration, operational support, and maintenance of the infrastructure of the service provided through the Botmaker platform in its software as a service (SaaS) format. Taking into consideration the protection of personal data that may be stored, transmitted, or processed.

which fulfils the requirements of the following standard;

ISO/IEC 27701:2019

Issued on: **31/10/2025**
Expires on: **31/10/2028**

Registration Number: **AR - PIM - 1**

Alex Stoichitoiu
President of IQNET

Gustavo Pontoriero
Certification Division Manager

IRAM Instituto Argentino de Normalización y Certificación

This attestation is directly linked to the IQNET Member's original certificate and shall not be used as a stand-alone document.

IQNET Members*:
AENOR Spain **AFNOR Certification** France **APCER** Portugal **CCC** Cyprus **CISQ** Italy **CQC** China **CQM** China **CQS** Czech Republic **Cro Cert** Croatia **DQS Holding GmbH** Germany **EAGLE Certification Group** USA **FCAV** Brazil **FONDONORMA** Venezuela **ICONTEC** Colombia **ICS** Bosnia and Herzegovina **Inspecta Sertifiointi Oy** Finland **INTECO** Costa Rica **IRAM** Argentina **JQA** Japan **KFQ** Korea **LSQA** Uruguay **MIRTEC** Greece **MSZT** Hungary **Nemko AS** Norway **NSAI** Ireland **NYCE-SIGE** México **PCBC** Poland **Quality Austria** Austria **SII** Israel **SIQ** Slovenia **SIRIM QAS International** Malaysia **SQS** Switzerland **SRAC** Romania **TSE** Turkey **YUQS** Serbia

* The list of IQNET Members is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

CERTIFICADO DE SISTEMAS DE GESTIÓN

Miembro de IQNET

IRAM certifica que:

BOTMAKER ARGENTINA - BOTMAKER S.R.L. / BOTMAKER USA - BOTMAKER INC / BOTMAKER BRASIL - BM BRASIL INTERNET LTDA.

Casa central: Virrey Olaguer y Feliú 2535 - (C1426EBC) - Ciudad Autónoma de Buenos Aires - República Argentina
Sitio Brasil: R. Pirandello 45 - (04623-000) - São Paulo - República Federativa do Brasil
Sitio EEUU: 3390 Mary St Suite 310 - (33131) - Miami - Florida - Estados Unidos de América

posee un **Sistema de Gestión de la Información de Privacidad** que cumple con los requisitos de la norma:

ISO/IEC 27701:2019

Registro N.º 27700-1

Cuyo alcance es:

Administración, soporte operativo y mantenimiento de la infraestructura del servicio brindado a través de la plataforma Botmaker en su modalidad de "Software as a Service" (SaaS). Teniendo en cuenta la protección de los datos personales que pudieran almacenarse, transmitirse o procesarse.

Emisión: 10/11/2025

Vigencia: 31/10/2025 a 31/10/2028

Gustavo Pontoriero
Gerente de División SG&CP
Certificación IRAM
(Firmado digitalmente)

Este certificado es válido siempre que la organización mantenga en operación, en condiciones satisfactorias, su Sistema de Gestión de la Información de Privacidad y que cumpla con el acuerdo de certificación DC-R 010 y el manual DC-PG 096.

DC-FL 069

botmaker
UNLEASH HUMAN POTENTIAL

DECLARAÇÃO DE NÃO DESCONTINUIDADE

BM BRASIL INTERNET LTDA, CNPJ nº 30.607.960/0001-85, Endereço: Rua Surubim, 577, Conjuntos 171 e 172, 17º andar – Cidade Monções – São Paulo/SP – CEP 04571-050, declara para os devidos fins que:

1. **Todos os componentes, módulos, APIs, serviços, funcionalidades e versões** que compõem a solução **Botmaker** ofertada ao BANRISUL — incluindo mensageria omnichannel, fluxos, automações, integrações, inteligência artificial, infraestrutura, segurança e recursos administrativos — **não estão inseridos em listas de descontinuidade** da fabricante.
2. **Não há previsão de descontinuidade**, alteração de suporte, fim de ciclo de vida (EoL), fim de suporte (EoS) ou qualquer mudança que comprometa o pleno funcionamento da solução **do momento da entrega da proposta até os 12 (doze) meses subsequentes**.
3. A Botmaker adota processos formais de **gestão de produto**, **ciclo de vida tecnológico**, **roadmap estruturado** e **governança de releases**, assegurando estabilidade, manutenção contínua e evolução incremental de seus componentes.
4. Caso qualquer item venha a sofrer alteração em seu ciclo de vida, a Botmaker compromete-se a:
    - Comunicar formalmente o BANRISUL com **antecedência mínima de 90 dias**;
    - Disponibilizar **planos de migração, atualização ou substituição**, garantindo continuidade operacional;
    - Manter **suporte técnico integral** durante a transição.

5. Esta declaração é emitida com base nas políticas internas corporativas e nos processos de garantia de continuidade tecnológica da plataforma.

Ficamos à disposição para mais informações.

São Paulo, SP
27/11/2025

Felipe David Cohen
LICITANTE

Telefone: 11 97215-5971
E-mail:felipe.cohen@botmaker.io

Clicksign 518d84dd-7196-4f81-8639-c2b804df3473

DECLARAÇÃO DE NÃO DESCONTINUIDADE.pdf

Documento número #518d84dd-7196-4f81-8639-c2b804df3473

Hash do documento original (SHA256): 584e111814eb326978a66695df696b3874af8a7e2c8e93a3b87a2afb925e3495

Assinaturas

Felipe Cohen
Assinou como representante legal em 27 nov 2025 às 14:23:33

Log

27 nov 2025, 14:21:50	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 criou este documento número 518d84dd-7196-4f81-8639-c2b804df3473. Data limite para assinatura do documento: 27 de dezembro de 2025 (14:21). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
27 nov 2025, 14:22:47	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Data limite para assinatura do documento: 28 de novembro de 2025 (14:36).
27 nov 2025, 14:22:47	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 adicionou à Lista de Assinatura: felipe.cohen@botmaker.io para assinar como representante legal, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Felipe Cohen.
27 nov 2025, 14:23:33	Felipe Cohen assinou como representante legal. Pontos de autenticação: Token via E-mail felipe.cohen@botmaker.io. IP: 177.115.61.208. Localização compartilhada pelo dispositivo eletrônico: latitude -23.57487142476087 e longitude -46.66709795430185. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1352.1 disponibilizado em https://app.clicksign.com.
27 nov 2025, 14:23:34	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 518d84dd-7196-4f81-8639-c2b804df3473.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 518d84dd-7196-4f81-8639-c2b804df3473, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

Google Confidental Information

CSAP-2025-002호

보 안 인 증 서

업체명 : Google LLC　　대표자명 : Sundar Pichai

보안인증 대상 : 구글 클라우드 플랫폼
(GCP, 하등급, 다 그룹 용) (IaaS 하등급)

보안인증 유효기간 : 5년(2025. 1. 22. ~ 2030. 1. 21.)

「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2 제1항 및 같은 법 시행령 제15조의6제7항에 따라 위와 같이 클라우드컴퓨팅서비스에 대해 보안인증합니다.

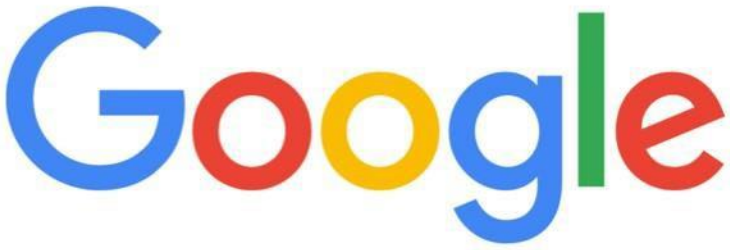
※ 단, 국가·공공기관 대상 서비스 제공 시 「사이버안보 업무규정」 제9조에 따른 국가정보원의 추가 검증 필요

2025년 1월 22일

클라우드 서비스 보안인증 CSAP Cloud Security Assurance Program

KISA 한국인터넷진흥원장

한국인터넷진흥원장의인



System and Organization Controls (SOC) 3

Report over the Google Cloud Platform System

Relevant to Security, Availability, Confidentiality, And Privacy

For the Period 01 August 2024 to 31 July 2025

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Google Cloud Platform System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy

We, as management of Google LLC ("Google" or "the Company") are responsible for:

- Identifying the Google Cloud Platform (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our service commitments and system requirements
- Identifying the risks that would threaten the achievement of our service commitments and system requirements that are the objectives of our System, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements
- Selecting the trust services categories and associated criteria that are the basis of our assertion

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period 1 August 2024 to 31 July 2025, to provide reasonable assurance that the service commitments and system requirements were achieved, based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Very truly yours,

Google LLC
18 September 2025

Shape the future
with confidence

Ernst & Young LLP
303 Almaden Blvd
San Jose, CA 95110

Tel: +1 949 794 2300
Fax: +1 866 492 5140
ey.com

Report of Independent Service Auditor's Report

To the Management of Google LLC:

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of Its Controls Over the Google Cloud Platform System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy" (Assertion), that Google's controls over the Google Cloud Platform System (System) were effective throughout the period 1 August 2024 to 31 July 2025, to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria.*

Management's Responsibilities

Google's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Google's service commitments and system requirements were achieved. Google's management is also responsible for providing the accompanying assertion about the effectiveness of controls within the System, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and service requirements that are the objectives of the System.

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Google's relevant security, availability, confidentiality, and privacy policies, processes, and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Google's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Our examination was also not conducted for the purpose of evaluating the performance or integrity of Google's AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Google's AI services.

We are required to be independent of Google and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA. We have complied with such independence and other ethical requirements and applied the AICPA's Statements on Quality Control Standards.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Google's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent

Shape the future with confidence

attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Google's controls over the System were effective throughout the period 1 August 2024 to 31 July 2025, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

18 September 2025
San Jose, CA

Attachment A - Google Cloud Platform System

Overview

Google LLC (“Google” or “the Company”), an Alphabet subsidiary, is a global technology service provider focused on improving the ways people connect with information. Google’s innovations in web search and advertising have made Google’s website one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world’s largest online index of websites and other content, and makes this information freely available to anyone with an Internet connection. Google’s automated search technology helps people obtain nearly instant access to relevant information from their vast online index.

Google Cloud Platform provides Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) and, allowing businesses and developers to build and run any or all of their applications on Google’s Cloud infrastructure. Customers can benefit from the performance, scale, reliability, ease-of-use, and a pay-as-you-go cost model.

Google’s product offerings for Google Cloud Platform (GCP) provide the unique advantage of leveraging the resources of Google’s core engineering team while also having a dedicated team to develop solutions for the corporate market. As a result, these Google offerings are positioned to innovate at a rapid rate and provide the same level of service that users are familiar with on google.com.

This report only applies to the underlying infrastructure and systems that support the services outlined below. The examination was also not conducted for the purpose of evaluating the performance or integrity of Google’s AI services or models.

Google Cloud Platform includes the following services, hereafter described collectively as “Google Cloud Platform” or "GCP":

- Artificial Intelligence (AI) and Machine Learning (ML) - Innovative, scalable machine learning services, with pre-trained models and the ability to generate tailored models
- Application Programming Interface (API) Management - Develop, deploy, and manage APIs on any Google Cloud back end
- Compute - A range of computing options tailored to match the size and needs of any organization
- Data Analytics - Tools to capture, process, store and analyze data on a single platform
- Databases - Migrate, manage, and modernize data with secure, reliable, and highly available relational and nonrelational databases
- Developer Tools - A collection of tools and libraries that help development teams work more quickly and effectively
- Healthcare and Life Sciences - Healthcare solution to protect sensitive data and maintain compliance with numerous requirements across various domains, geographies, and workloads

- Hybrid and Multi-cloud - Connect on-premises or existing cloud infrastructure with Google Cloud's scalability and innovation
- Management Tools - Manage apps on GCP with a web-based console, mobile app, or Cloud Shell for real time monitoring, logging, diagnostics, and configuration
- Media and Gaming - Build user experiences and empower developers by minimizing infrastructure complexity and accelerating data insights
- Migration - Large-scale, secure online data transfers to Cloud Storage and databases
- Networking - A private network using software-defined networking and distributed systems technologies to host and deliver services around the world
- Operations - Suite of products to monitor, troubleshoot, and improve application performance on Google Cloud environments
- Security and Identity - Manage the security and access to cloud assets, supported by Google's own protection of its infrastructure
- Serverless Computing - Deploy functions or apps as source code or as containers without worrying about the underlying infrastructure. Build full stack serverless applications with Google Cloud's storage, databases, machine learning, and more
- Storage - Scalable storage options and varieties for different needs and price points
- Other - Additional GCP services supporting e-commerce, procurement, billing, and petabyte-scale scientific analysis and visualization of geospatial datasets

The Google Cloud Platform products covered in this system description consist of the following services:

- Artificial Intelligence (AI) and Machine Learning (ML)
- Agent Assist
- Agentspace[5]
- AI Platform Deep Learning Container
- AI Platform Training and Prediction[3]
- Anti-Money Laundering (AML) AI
- AutoML Tables
- AutoML Translation
- Cloud Natural Language API
- Cloud Speaker ID
- Cloud Translation
- Cloud Vision
- Conversational AI (formerly Contact Center AI (CCAI)
- Conversational Insights (formerly Contact Center AI Insights)
- Dialogflow
- Document AI
- Document AI Warehouse
- Food Ordering AI Agent

- Gemini Code Assist[5]
- Gemini for Google Cloud
- Gemini in BigQuery[5]
- Generative AI on Vertex AI
- Google Cloud Contact Center as a Service (CCaaS)
- NotebookLM for Enterprise[5]
- Ray on Vertex AI
- Recommendations AI
- Retail Search
- Speech-to-Text
- Talent Solution
- Text-to-Speech
- Vertex AI Codey[4]
- Vertex AI Colab Enterprise
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Vertex AI Workbench Instances
- Video Intelligence API

- Application Programming Interface (API) Management
  - Advanced API Security
  - Apigee
  - API Gateway
  - Application Integration
  - Cloud Endpoints
  - Integration Connectors

- Compute
  - App Engine
  - Batch
  - Compute Engine
  - Workload Manager

- Data Analytics
  - BigQuery
  - Cloud Composer
  - Cloud Data Fusion
  - Cloud Life Sciences

    - Data Catalog
    - Dataflow
    - Dataform
    - Dataplex
    - Dataproc
    - Dataproc Metastore
    - Looker (Google Cloud core)
    - Looker Studio
    - Managed Service for Apache Kafka[1]
    - Pub/Sub
- Databases
    - AlloyDB
    - Cloud Bigtable
    - Cloud Spanner
    - Cloud SQL
    - Datastore
    - Firestore
    - Memorystore
- Developer Tools
    - Artifact Analysis
    - Artifact Registry
    - Cloud Build
    - Cloud Source Repositories
    - Cloud Workstations
    - Container Registry
    - Firebase Test Lab
    - Google Cloud Deploy
    - Google Cloud SDK
    - Infrastructure Manager
    - Secure Source Manager
- Healthcare and Life Sciences
    - Cloud Healthcare
    - Healthcare Data Engine (HDE)
- Hybrid and Multi-cloud
    - Connect

    - Google Kubernetes Engine
    - GKE Enterprise Config Management
    - GKE Identity Service
    - Hub
    - Knative serving
    - Service Mesh
- Management Tools
    - Cloud Console
    - Cloud Console App
    - Cloud Deployment Manager
    - Cloud Shell
    - Recommender
    - Service Infrastructure
- Media and Gaming
    - Media CDN
    - Transcoder API
- Migration
    - BigQuery Data Transfer Service
    - Database Migration Service
    - Migration Center
    - Migrate to Virtual Machines
    - Storage Transfer Service
- Networking
    - Cloud CDN
    - Cloud DNS
    - Cloud IDS (Cloud Intrusion Detection System)
    - Cloud Interconnect
    - Cloud Load Balancing
    - Cloud Network Address Translation (NAT)
    - Cloud NGFW
    - Cloud Router
    - Cloud Service Mesh
    - Cloud Virtual Private Network (VPN)
    - Google Cloud Armor
    - Network Connectivity Center

  - Network Intelligence Center
  - Network Service Tiers
  - Service Directory
  - Spectrum Access System
  - Traffic Director
  - Virtual Private Cloud (VPC)
- Operations
  - Cloud Logging
  - Cloud Monitoring
  - Cloud Profiler
  - Cloud Trace
  - Google Cloud Backup and DR
  - Personalized Service Health
- Security and Identity
  - Access Approval
  - Access Context Manager
  - Access Transparency
  - Assured Workloads
  - Binary Authorization
  - Certificate Authority Service
  - Certificate Manager
  - Chrome Enterprise Premium
  - Cloud Asset Inventory
  - Cloud External Key Manager (Cloud EKM)
  - Cloud Hardware Security Module (HSM)
  - Cloud Key Management Service (KMS)
  - Firebase App Check
  - Firebase Authentication
  - Google Cloud Identity-Aware Proxy
  - Google Threat Intelligence[2]
  - Google Security Operations (SIEM)[2]
  - Google Security Operations (SOAR)[2]
  - GTI for Google Security Operations[2]
  - Identity & Access Management (IAM)
  - Identity Platform
  - Key Access Justifications (KAJ)
  - Managed Service for Microsoft Active Directory (AD)

- Organization Policy[1]
- Privileged Access Manager
- reCAPTCHA Enterprise
- Resource Manager API
- Risk Manager
- SecLM
- Secret Manager
- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- VirusTotal
- VPC Service Controls
- Web Risk API

- Serverless Computing
  - Cloud Functions
  - Cloud Functions for Firebase
  - Cloud Run
  - Cloud Scheduler
  - Cloud Tasks
  - Datastream
  - Eventarc
  - Workflows

- Storage
  - Backup for GKE
  - Cloud Filestore
  - Cloud Storage
  - Cloud Storage for Firebase
  - Parallelstore[1]
  - Persistent Disk

- Other
  - Cloud Billing
  - Google Earth Engine
  - Google Cloud Marketplace
  - Google Cloud Skills Boost[1]
  - Tables

[1] Indicates products in scope only for the period 1 March 2025 through 31 July 2025

[2] Google Security Operations (SIEM), Google Security Operations (SOAR) and Google Threat Intelligence (GTI) for Google Security Operations are covered by separate terms than GCP. Refer to the Terms of Services (https://cloud.google.com/terms/secops/service-terms) for additional details

[3]The AI Platform Training & Prediction product was deprecated on January 31, 2025.

[4]The Vertex AI Codey product was deprecated on April 21, 2025.

[5] Indicates products in scope only for the period 1 May 2025 through 31 July 2025

The products are composed of communication, productivity, collaboration, and security tools that can be accessed from virtually any location with secure Internet connectivity. This means every employee and each user entity they work with can be productive from anywhere, using any device with a secure Internet connection.

These products provide a comprehensive variety of technical services that organizations rely on:

Artificial Intelligence (AI) and Machine Learning (ML)

Google does not use Customer Data to train or fine-tune any AI/ML models without a customer's prior permission or instruction. Refer to the service terms (https://cloud.google.com/terms/service-terms) for additional details.

Agent Assist

Agent Assist is a Large Language Model (LLM)- powered AI solution that increases human agent productivity and enhances customer service by offering real-time assistance.

Agentspace

Agentspace combines AI Agents, Gemini models, and Google search technologies to enable automation and enhance employee productivity by connecting enterprise data sources and applications, offering workflow automation, search functionality, and generative AI features.

AI Platform Deep Learning Container

AI Platform Deep Learning Container provides Docker images with AI frameworks that can be customized and used with Google Kubernetes Engine (GKE), Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.

AI Platform Training and Prediction

AI Platform Training and Prediction is a managed service that enables users to easily build machine learning models with popular frameworks like TensorFlow, XGBoost and Scikit Learn. It provides scalable training and prediction services that work on large datasets.

Anti-Money Laundering (AML) AI

AML AI is a machine learning engine which takes customer data and training labels to create a tailored model covering an extensible typology of risks for AML along with governance documentation to ease adoption in this highly regulated environment.

AutoML Tables

AutoML Tables enables data scientists, analysts, and developers to automatically build and deploy machine learning models on structured data at increased speed and scale.

AutoML Translation

AutoML Translation is a simple and scalable translation solution that allows businesses and developers with limited machine learning expertise to customize the Google Neural Machine Translation (GNMT) model for their own domain or use-case.

Cloud Natural Language API

Cloud Natural Language API provides natural language understanding as a simple to use Application Programming Interface (API). Given a block of text, this API enables finding entities, analyzing sentiment (positive or negative), analyzing syntax (including parts of speech and dependency trees), and categorizing the content into a rich taxonomy. The API can be called by passing the content directly or by referring to a document in Cloud Storage.

Cloud Speaker ID

Speaker ID allows customers to enroll user voice prints and later verify users against a previously enrolled voice print.

Cloud Translation

Cloud Translation automatically translates text from one language to another language (e.g., French to English). The API is used to programmatically translate text in webpages or apps.

Cloud Vision

Cloud Vision enables the understanding of image content by encapsulating machine learning models in a Representational State Transfer (REST) API. It classifies images into thousands of categories, detects individual objects and faces within images, and finds and reads printed words contained within images. It can be applied to build metadata on image catalogs, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. It can also analyze images uploaded in the request and integrate with image storage on Google Cloud Storage.

Conversational AI (formerly Contact Center AI (CCAI)

Conversational AI uses AI to improve the customer experience in contact centers. It includes Agent Assist, Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Insights, Speech-to-Text, Text-to-Speech, and Speaker ID.

Conversational Insights (formerly Contact Center AI Insights)

Conversational Insights helps customers extract value from their contact center data by identifying sentiment and topics and highlighting key insights in the data.

Dialogflow

Dialogflow is a development suite for voice and text conversational apps including chatbots. Dialogflow is cross-platform and can connect to apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Actions on Google, Facebook Messenger, Slack).

Document AI

Document AI classifies and extracts structured data from documents to help streamline data validation and automate business processes.

Document AI Warehouse

Document AI Warehouse is a data management and governance platform that stores, searches, and organizes documents and their extracted and tagged metadata. Document AI Warehouse is highly scalable and fully managed and can be integrated with enterprise document workflows, applications, and repositories.

Food Ordering AI Agent

A repeatable, scalable Food Ordering Voice Assistant that helps restaurants serve their customers with high quality and consistent service.

Google Cloud Contact Center as a Service (CCaaS)

Google Cloud CCaaS is a contact-center-as-a-service (CCaaS) platform leveraging Conversational AI. It integrates directly with CRMs and queues and routes customer interactions across voice and digital channels to resource pools, including human agents.

Gemini Code Assist

Gemini Code Assist provides AI-powered assistance to help customer development teams build, deploy, and operate applications throughout the software development lifecycle.

Gemini for Google Cloud

Gemini for Google Cloud provides AI-powered end user assistance with a wide range of Google Cloud products. Gemini for Google Cloud is a generative AI-powered collaboration Service that provides assistance to Google Cloud end users. Gemini for Google Cloud is embedded in many Google Cloud products to provide developers, data scientists, and operators an integrated assistance experience.

Gemini in BigQuery

Gemini in BigQuery provides AI-powered assistance to help customers understand, query, and work with their data across the entire data lifecycle.

Generative AI on Vertex AI

Generative AI on Vertex AI includes features for generative AI use cases, including large language, text-to-image, and image-to-text models.

NotebookLM for Enterprise

NotebookLM for enterprise enables customers to use generative AI to summarize and extract information from their data.

Ray on Vertex AI

Ray on Vertex AI is an open-source framework for scaling AI and Python applications. Ray provides the infrastructure to perform distributed computing and parallel processing for the user's machine learning (ML) workflow.

Recommendations AI

Recommendations AI enables customers to build a personalized recommendation system using ML models.

Retail Search

Retail Search allows retailers to leverage Google's search capabilities on their retail websites and applications.

Speech-to-Text

Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy-to-use API.

Talent Solution

Talent Solution offers access to Google's machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.

Text-to-Speech

Text-to-Speech synthesizes human-like speech based on input text in a variety of voices and languages.

Vertex AI Codey

Vertex AI Codey is a suite of models that work with code that includes the following APIs:

- The code generation API - Generates code based on a natural language description of the desired code.
- The code chat API - Can power a chatbot that assists with code-related questions.
- The code completion API - Provides code autocompletion suggestions as users write code.

Vertex AI Colab Enterprise

Vertex AI Colab Enterprise is a collaborative, managed notebook environment with the security and compliance capabilities of Google Cloud.

Vertex AI Conversation

Vertex AI Conversation allows customers to leverage foundational models and conversational AI to create multimodal chat or voice agents.

Vertex AI Platform

Vertex AI Platform is a service for managing the AI and machine learning development lifecycle. Customers can (i) store and manage datasets, labels, features, and models; (ii) build pipelines to train and evaluate models and run experiments using Google Cloud algorithms or custom training code; (iii) deploy models for online or batch use cases; (iv) manage data science workflows using Colab Enterprise and Vertex AI Workbench (also known as Notebooks); and (v) create business optimization plans with Vertex Decision Optimization.

Vertex AI Search

Vertex AI Search allows customers to leverage foundational models and search and recommendation technologies to create multimodal semantic search and question-answering experiences.

Vertex AI Workbench Instances

Vertex AI Workbench instances are Jupyter notebook-based development environments for the entire data science workflow. Users can interact with Vertex AI and other Google Cloud services from within a Vertex AI Workbench instance's Jupyter notebook.

Video Intelligence API

Video Intelligence API makes videos searchable, and discoverable, by extracting metadata through a REST API. It annotates videos stored in Google Cloud Storage and helps identify key noun entities in a video and when they occur within the video.

API Management

Advanced API Security

Advanced API Security acts as the users' API's vigilant guardian. It constantly analyzes incoming traffic, seeking out anomalous patterns that might indicate attacks or abuse. When suspicious activity is spotted, it can block harmful requests or alert users for further action. Additionally, it evaluates the users' API setups against security best practices, offering recommendations for improvement. This comprehensive approach helps users proactively safeguard the users' APIs, protect sensitive data, and ensure the users' API configurations are designed to withstand security challenges.

Apigee

Apigee is a full-lifecycle API management platform that lets customers design, secure, analyze, and scale APIs, giving them visibility and control. Apigee is available as Apigee, a fully managed service, Apigee hybrid, a hybrid model that's partially hosted and managed by the customer, or Apigee Private Cloud, an entirely customer hosted Premium Software solution. Apigee Private Cloud is not in scope for this report.

API Gateway

API Gateway is a fully managed service that enables users to develop, deploy, and secure APIs running on Google Cloud Platform.

Application Integration

Application Integration is an Integration-Platform-as-a-Service (iPaaS) that offers a comprehensive set of integration tools to connect and manage the multitude of applications and data required to support various business operations. Application Integration provides a unified drag and drop integration designer interface, triggers that help invoke an integration, configurable tasks and numerous connectors that allow connectivity to business applications, technologies, and other data sources using the native protocols of each target application.

Cloud Endpoints

Cloud Endpoints is a tool that provides services to develop, deploy, secure and monitor APIs running on Google Cloud Platform.

Integration Connectors

Integration Connectors is a platform that allows customers to connect to business applications, technologies and other data sources using native protocols of each target application. The connectivity established through these connectors helps manage access to various data sources which can be used with other services like Application Integration through a consistent, standard interface.

Compute

App Engine

App Engine enables the building and hosting of web apps on the same systems that power Google applications. App Engine offers fast development and deployment of applications without the need to manage servers or other low-level infrastructure components. Scaling and software patching are handled by App Engine on the user's behalf. App Engine also provides the ability to create managed virtual machines (VMs). In addition, client APIs can be built for App Engine applications using Google Cloud Endpoints.

Batch

Batch is a fully managed service that lets users schedule, queue, and execute batch processing workloads on Compute Engine virtual machine (VM) instances. Batch provisions resources and manages capacity on users' behalf, allowing user batch workloads to run at scale.

Compute Engine

Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud. With virtual machines that can boot in minutes, it offers many configurations including custom machine types that can be optimized for specific use cases as well as support for Graphics Processing Units (GPUs), Tensor Processing Units (TPUs) and Local Solid-State Drive (SSD). Additionally, customers can enable Shielded VMs to provide advanced platform security.

Workload Manager

Workload Manager is a rule-based validation service for evaluating workloads running on Google Cloud. If enabled, Workload Manager scans application workloads to detect deviations from standards, rules, and best practices that improve system quality, reliability, and performance.

Data Analytics

BigQuery

BigQuery is a fully managed, petabyte-scale analytics data warehouse that features scalable data storage and the ability to perform ad hoc queries on multi-terabyte datasets. BigQuery allows users to share data insights via the web and control access to data based on business needs.

Cloud Composer

Cloud Composer is a managed workflow orchestration service that can be used to author, schedule, and monitor pipelines that span across clouds and on-premises data centers.

Cloud Data Fusion

Cloud Data Fusion is a fully managed, cloud native, enterprise data integration service for building and managing data pipelines. Cloud Data Fusion provides a graphical interface that allows customers to build scalable data integration solutions to cleanse, prepare, blend, transfer, and transform data.

Cloud Life Sciences

Cloud Life Sciences is a suite of services and tools to store, process, inspect and share biomedical data, DNA sequence reads, reference-based alignments, and variant calls, using Google's cloud infrastructure.

Data Catalog

Data Catalog is a fully managed and scalable metadata management service that allows organizations to have a centralized and unified view of data assets.

Dataflow

Dataflow is a fully managed service for consistent, parallel data-processing pipelines. It utilizes the Apache Beam Software Development Kits (SDKs) with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the lifecycle of Compute Engine resources for the processing pipeline(s) and provides a monitoring interface for understanding pipeline health.

Dataform

Dataform is a service for data analysts to develop, test, version control, and schedule complex SQL workflows for data transformation in BigQuery. Dataform lets users manage data transformation in the Extraction, Loading, and Transformation (ELT) process for data integration. After raw data is extracted from source systems and loaded into BigQuery, Dataform helps users to transform it into a well-defined, tested, and documented suite of data tables.

Dataplex

Dataplex is an intelligent data fabric that helps customers unify distributed data and automate management and governance across that data to power analytics at scale.

Dataproc

Dataproc is a managed service for distributed data processing. It provides management, integration, and development tools for deploying and using Apache Hadoop, Apache Spark, and other related open source data processing tools. With Cloud Dataproc, clusters can be created and deleted on-demand and sized to fit whatever workload is at hand.

Dataproc Metastore

Dataproc Metastore provides a fully-managed metastore service that simplifies technical metadata management and is based on a fully-featured Apache Hive metastore. Dataproc Metastore can be used as a metadata storage service component for data lakes built on open source processing frameworks like Apache Hadoop, Apache Spark, Apache Hive, Presto, and others.

Looker (Google Cloud core)

Looker (Google Cloud core) is a business intelligence and embedded analytics solution hosted on Google infrastructure. With Looker (Google Cloud core), customers can build semantic models using various data sources, develop customized insights from the models, and share those insights for collaboration via dashboards and other services.

Looker Studio

Looker Studio is a visualization and business intelligence product that enables users to connect to multiple datasets and turn their data into informative, easy to share, and fully customizable dashboards and reports.

Managed Service for Apache Kafka

Managed Service for Apache Kafka is a Google Cloud service that helps you run secure, scalable open source Apache Kafka clusters.

Pub/Sub

Pub/Sub provides reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a topic while other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Cloud Pub/Sub allows communication between independent applications.

Databases

AlloyDB

AlloyDB is an enterprise grade database product that combines the familiarity of open source DB front-ends, like PostgreSQL, with custom-built storage, query and connectivity layers for superior availability, performance, security and manageability.

Cloud Bigtable

Cloud Bigtable is a low-latency, fully managed, highly scalable NoSQL database service. It is designed for the retention and serving of data from gigabytes to petabytes in size.

Cloud Spanner

Cloud Spanner is a fully managed, scalable, relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and ACID (Atomicity, Consistency, Isolation, Durability) transactions with synchronous replication of data across regions.

Cloud SQL

Cloud SQL is a service to create, configure, and use managed third-party relational databases in Google Cloud Platform. Cloud SQL maintains, manages, and administers those databases.

Datastore

Datastore is a highly scalable NoSQL database for mobile and web applications. It provides query capabilities, atomic transitions, index, and automatically scales up and down in response to load.

Firestore

Firestore is a fully managed, scalable, serverless NoSQL document database for mobile, web, and server development. It provides query capabilities, live synchronization, and offline support.

Memorystore

Memorystore for Redis (Remote Dictionary Server) provides a fully managed in-memory data store service for GCP. Cloud Memorystore can be used to build application caches that provide

low latency data access. Cloud Memorystore is compatible with the Redis protocol, allowing seamless migration with no code changes.

Developer Tools

Artifact Analysis

Artifact Analysis is a family of services that provide software composition analysis, metadata storage and retrieval. Its detection points are built into a number of Google Cloud products such as Artifact Registry and Google Kubernetes Engine (GKE) for quick enablement. The service works with both Google Cloud's first-party products and also lets users store information from third-party sources. The scanning services leverage a common vulnerability store for matching files against known vulnerabilities.

Artifact Registry

Artifact Registry is a service for managing container images and packages. It is integrated with Google Cloud tooling and runtimes and comes with support for native artifact protocols. This makes it simple to integrate it with user CI/CD tooling to set up automated pipelines.

Cloud Build

Cloud Build allows for the creation of container images from application source code located in Cloud Storage or in a third-party service (e.g., Github, Bitbucket). Created container images can be stored in Container Registry and deployed on Container Engine, Compute Engine, App Engine Flexible Environment, or other services to run applications from Docker containers.

Cloud Source Repositories

Cloud Source Repositories provides Git version control to support collaborative development of any application or service as well as a source browser that can be used to browse the contents of repositories and view individual files from within the Cloud Console. Cloud Source Repositories and related tools (e.g., Cloud Debugger) can be used to view debugging information alongside code during application runtime.

Cloud Workstations

Cloud Workstations provides preconfigured, customizable, and secure managed development environments on Google Cloud. Cloud Workstations is accessible through a browser-based Integrated Development Environment (IDE), from multiple local code editors (such as IntelliJ IDEA Ultimate or VS Code), or through SSH. Instead of manually setting up development environments, users can create a workstation configuration specifying user environments in a reproducible way.

Container Registry

Container Registry is a private Docker image storage system on Google Cloud Platform.

Firebase Test Lab

Firebase Test Lab provides cloud-based infrastructure for testing apps on physical and virtual devices. Developers can test their apps across a wide variety of devices with Firebase Test Lab.

Google Cloud Deploy

Google Cloud Deploy is a managed service that automates delivery of user applications to a series of target environments in a defined promotion sequence. When users want to deploy updated applications, users create a release, whose lifecycle is managed by a delivery pipeline.

Google Cloud SDK

Google Cloud SDK is a set of tools to manage resources and applications hosted on Google Cloud Platform. It includes the Google Cloud Command Line Interface (CLI), Cloud Client Libraries for programmatic access to Google Cloud Platform services, the gsutil, kubectl, and bq command line tools, and various service and data emulators for local platform development. The Google Cloud SDK provides the primary programmatic interfaces to Google Cloud Platform.

Infrastructure Manager

Infrastructure Manager is a managed service that automates the deployment and management of Google Cloud infrastructure resources. Infrastructure is defined using Terraform and deployed onto Google Cloud by Infra Manager, enabling users to manage resources using Infrastructure as Code (IaC).

Secure Source Manager

Secure Source Manager is a fully-managed service that provides a Git-based source code management system.

Healthcare and Life Sciences

Cloud Healthcare

Cloud Healthcare provides managed services and an API to store, process, manage, and retrieve healthcare data in a variety of industry standard formats.

Healthcare Data Engine (HDE)

HDE is a solution that enables (1) harmonization of healthcare data to the Fast Healthcare Interoperability Resources (“FHIR”) standard and (2) streaming of healthcare data to an analytic environment.

Hybrid and Multi-cloud

The scope of the services included in this report is limited to the services managed by Google and does not extend to the application of the services in other cloud service providers' environments by the user entity. Refer to the Terms of Services (https://cloud.google.com/terms/services) for additional details.

Connect

Connect is a service that allows users to connect Kubernetes clusters to Cloud. This enables both users and Google-hosted components to interact with clusters through a connection to the in-cluster Connect software agent.

Google Kubernetes Engine

Google Kubernetes Engine, powered by the open source container scheduler Kubernetes, runs containers on Google Cloud Platform. Kubernetes Engine manages provisioning and maintaining the underlying virtual machine cluster, scaling applications, and operational logistics such as logging, monitoring, and cluster health management.

GKE Enterprise Config Management

GKE Enterprise Config Management is a policy management solution for enabling consistent configuration across multiple Kubernetes clusters. GKE Enterprise Config Management allows customers to specify one single source of truth and then enforce those policies on the clusters.

GKE Identity Service

GKE Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple environments. Users can log in to and access their clusters from the command line or from the Cloud Console, all using their existing identity providers.

Hub

Hub is a centralized control-plane that enables a user to centrally manage features and services on customer-registered clusters running in a variety of environments, including Google’s cloud, on-premises in customer data centers, or other third-party clouds.

Knative serving

Knative serving is Google's managed and fully supported Knative offering. Knative serving abstracts away the complexity of Kubernetes, making it easy to build and deploy user’s serverless workloads across hybrid and multi-cloud environments.

Service Mesh

Service Mesh is a managed service mesh service that includes (i) a managed certificate authority that issues cryptographic certificates that identify customer workloads within the Service Mesh for mutual authentication, and (ii) telemetry for customers to manage and monitor their services. Customers receive details showing an inventory of services, can understand their service dependencies, and receive metrics for monitoring their services. Service Mesh is provided as a service and as a software. The Service Mesh software offering is not in scope for this report.

Management Tools

Cloud Console

Cloud Console is a web-based interface used to build, modify, and manage services and resources on the Google Cloud Platform. Cloud services can be procured, configured, and run from Cloud Console.

Cloud Console App

Cloud Console App is a native mobile app that provides monitoring, alerting, and the ability to take actions on resources.

Cloud Deployment Manager

Cloud Deployment Manager is an infrastructure management service which automates creation, and management of Google Cloud Platform resources.

Cloud Shell

Cloud Shell provides command-line access to Google Cloud Platform resources through an in-browser Linux shell backed by a temporary Linux VM in the cloud. It allows projects and resources to be managed without having to install additional tools on systems and comes equipped and configured with common developer tools such as text editors, a MySQL client and Kubernetes.

Recommender

Recommender automatically analyzes usage patterns to provide recommendations and insights across services to help use Google Cloud Platform in a more secure, cost-effective, and efficient manner.

Service Infrastructure

Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services. It includes:

- Service Management API, which lets service producers manage their APIs and services;
- Service Consumer Management API, which lets service producers manage their relationships with their service consumers;
- Service Control API, which lets managed services integrate with Service Infrastructure for admission control and telemetry reporting functionality; and
- Service Usage API, which lets service consumers manage their usage of APIs and services

Media and Gaming

Media CDN

Media CDN is a planet-scale content delivery network allowing customers to automate all facets of deployment and management. Stream media and deliver exceptional experiences to customer end users, no matter where they are.

Transcoder API

Transcoder API can batch convert media files into optimized formats to enable streaming across web, mobile, and living room devices. It provides fast, easy to use, large-scale processing of advanced codecs while utilizing Google's storage, networking, and delivery infrastructure.

Migration

BigQuery Data Transfer Service

BigQuery Data Transfer Service automates data movement from Software as a Service (SaaS) applications to BigQuery on a scheduled, managed basis.

Database Migration Service

Database Migration Service is a fully managed migration service that enables users to perform high fidelity, minimal-downtime migrations at scale. Users can use Database Migration Service to migrate from on-premises environments, Compute Engine, and other clouds to certain Google Cloud-managed databases.

Migration Center

Migration Center provides tools, best practices and data-driven prescriptive guidance designed to accelerate the end-to-end cloud migration journey through business case development, environment discovery, workload mapping, migration planning, financial analysis, foundation setup and migration execution.

Migrate to Virtual Machines

Migrate to Virtual Machines is a fully-managed migration service that enables customers to migrate workloads at scale into Google Cloud Compute Engine with minimal down time by utilizing replication-based migration technology.

Storage Transfer Service

Storage Transfer Service provides the ability to import large amounts of online data into Google Cloud Storage. It can transfer data from Amazon Simple Storage Service (Amazon S3) and other HTTP/HTTPS locations as well as transfer data between Google Cloud Storage buckets.

Networking

Cloud CDN

Cloud Content Delivery Network (CDN) uses Google's distributed network edge points of presence to cache HTTP(S) load balanced content.

Cloud DNS

Cloud DNS is a fully managed Domain Name System (DNS) service which operates a geographically diverse network of high-availability authoritative name servers. Cloud DNS provides a service to publish and manage DNS records for applications and services.

Cloud IDS (Cloud Intrusion Detection System)

Cloud IDS is a managed service that aids in detecting certain malware, spyware, command-and-control attacks, and other network-based threats.

Cloud Interconnect

Cloud Interconnect offers enterprise-grade connections to Google Cloud Platform. This solution provides direct connection between on-premise networks and GCP Virtual Private Cloud.

Cloud Load Balancing

Cloud Load Balancing is a distributed, software-defined, managed service for all traffic (HTTP(S), TCP/SSL, and UDP) to computing resources. Cloud Load Balancing rapidly responds to changes in traffic, network, backend health and other related conditions.

Cloud Network Address Translation (NAT)

Cloud Network Address Translation (NAT) enables virtual machine instances in a private network to communicate with the Internet, without external IP addresses.

Cloud NGFW

Cloud NGFW is a fully distributed, cloud-native firewall service that evaluates incoming and outgoing traffic on a network, according to user-defined firewall rules in the policy.

Cloud Router

Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between a Virtual Private Cloud (VPC) network and an external network, typically an on-premise network.

Cloud Service Mesh

Cloud Service Mesh is a service mesh available on Google Cloud and across supported GKE Enterprise platforms. It supports services running on a range of computing infrastructures. Cloud Service Mesh is controlled by APIs designed for Google Cloud, for open source, or for both.

Cloud Virtual Private Network (VPN)

Cloud Virtual Private Network (VPN) provides connections between on-premises or other external networks to Virtual Private Clouds on GCP via an IPsec connection or can be used to connect two different Google managed VPN gateways.

Google Cloud Armor

Google Cloud Armor provides access control configurations and at-scale defenses to help protect infrastructure and applications against distributed denial-of-service (DDoS), application-aware and multi-vector attacks.

Network Connectivity Center

Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud that facilitates connecting a customer's resources to its cloud network.

Network Intelligence Center

Network Intelligence Center provides a single console for managing Google Cloud's comprehensive network monitoring, verification, and optimization platform across the Google Cloud, multi-cloud, and on-premises environments.

Network Service Tiers

Network Service Tiers enable the selection of different quality networks (tiers) for outbound traffic to the Internet: Standard Tier primarily utilizes third-party transit providers while Premium Tier leverages Google's private backbone and peering surface for egress.

Service Directory

Service Directory is a managed service that offers customers a single place to publish, discover and connect their services in a consistent way, regardless of their environment. Service Directory supports services in Google Cloud, multi-cloud and on-premises environments and can scale up to thousands of services and endpoints for a single project.

Spectrum Access System

Spectrum Access System enables users to access the Citizens Broadband Radio Service (CBRS) in the United States, the 3.5 GHz band that is available for shared commercial use. Users can use Spectrum Access System to register CBRS devices, manage CBRS deployments, and access a non-production test environment.

Traffic Director

Traffic Director is Google Cloud Platform's traffic management service for open-source service meshes.

Virtual Private Cloud (VPC)

Virtual Private Cloud is a comprehensive set of managed networking capabilities for Google Cloud resources including granular IP address range selection, routes and firewalls.

Operations

Cloud Logging

Cloud Logging is a hosted solution that helps users gain insight into the health, performance and availability of their applications running on Google Cloud Platform and other public cloud platforms. It includes monitor dashboards to display key metrics, define alerts and report on the health of cloud systems. The components of Cloud Logging that run on other public cloud platforms are not in scope for this report.

Cloud Monitoring

Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from certain Services, hosted uptime probes, application instrumentation, alert management, notifications and a variety of application components.

Cloud Profiler

Cloud Profiler continuously gathers and reports source-level performance information from production services. It provides key information to determine what functions in code consume the most memory and CPU cycles so insights can be gained on how code operates to improve performance and optimize computing resources.

Cloud Trace

Cloud Trace collects latency data from applications and displays it in the Google Cloud Platform Console. It automatically analyzes trace data to generate in-depth performance reports that help identify and locate performance bottlenecks.

Google Cloud Backup and DR

Google Cloud Backup and DR is a managed backup and disaster recovery service for centralized protection of workloads in Google Cloud.

Personalized Service Health

Personalized Service Health, which lets users identify Google Cloud service disruptions relevant to user's projects so users can manage and respond to them efficiently. These disruptions are called service health events and are available in the Google Cloud console and a variety of integration points.

Security and Identity

Access Approval

Access Approval allows customers to approve eligible manual, targeted access by Google administrators to their data or workloads prior to access being granted.

Access Context Manager

Access Context Manager allows customer administrators to define attribute-based access control for projects, apps and resources.

Access Transparency

Access Transparency captures near real-time logs of certain manual, targeted accesses by Google personnel, and provides them via Cloud Logging accounts.

Assured Workloads

Assured Workloads provides functionality to create security controls that are enforced on customer cloud environment and can assist with compliance requirements (e.g. FedRAMP Moderate compliance).

Binary Authorization

Binary Authorization helps customers ensure that only signed and explicitly authorized container images are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.

Certificate Authority Service

Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Customers can use Certificate Authority Service to create certificate authorities using Cloud KMS keys to issue, revoke, and renew subordinate and end-entity certificates.

Certificate Manager

Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the certificates.

Chrome Enterprise Premium

Chrome Enterprise Premium is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware and phishing attacks. Chrome Enterprise Premium is an integrated platform incorporating cloud-based services and software components.

Cloud Asset Inventory

Cloud Asset Inventory is a service that allows customers to view, monitor, and analyze cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.

Cloud External Key Manager (Cloud EKM)

Cloud EKM lets customers encrypt data in Google Cloud Platform with encryption keys that are stored and managed in a third-party key management system deployed outside Google's infrastructure.

Cloud Hardware Security Module (HSM)

Cloud HSM is a cloud-hosted Hardware Security Module (HSM) service for hosting encryption keys and performing cryptographic operations.

Cloud Key Management Service (KMS)

Cloud KMS is a cloud-hosted key management service that manages encryption for cloud services. It enables the generation, use, rotation, and destruction of encryption keys.

Firebase App Check

Firebase App Check provides a service that can help protect access to user's APIs with platform specific attestation that helps verify app identity and device integrity.

Firebase Authentication

Firebase Authentication is a fully managed user identity and authentication system providing backend services enabling sign-in and sign-up experiences for an application or service.

Google Cloud Identity-Aware Proxy

Google Cloud Identity-Aware Proxy (Cloud IAP) is a tool that helps control access to applications running on Google Cloud Platform based on identity and group membership.

Google Threat Intelligence

Google Threat Intelligence combines the unmatched depth of our Mandiant frontline expertise, the global reach of the VirusTotal community, and the breadth of visibility only Google can deliver, based on billions of signals across devices and emails. Google Threat Intelligence includes Gemini in Threat Intelligence, our AI-powered agent that provides conversational search across our vast repository of threat intelligence, enabling customers to gain insights and protect themselves from threats faster than ever before. The Attack Surface Management (ASM) and Digital Threat Monitoring (DTM) features of Google Threat Intelligence are Mandiant products and maintain equivalent certifications.

Google Security Operations (SIEM)

Google Security Operations Security Information and Event Management (SIEM) enables enterprise security teams to detect, investigate, and respond to threats at speed and scale. Chronicle SIEM does this by collecting security telemetry data, aggregating it, normalizing it, and applying threat intelligence to identify the highest priority threats.

Google Security Operations (SOAR)

Google Security Operations Security Orchestration, Automation and Response (SOAR) is a platform designed to help organizations detect, investigate, and respond to security threats in real-time. The platform is powered by Google Cloud's infrastructure and leverages the machine learning capabilities of Google to automate and streamline security workflows.

GTI for Google Security Operations

GTI for Google Security Operations is a service extension for Google Security Operations (SIEM) that hunts for threats in external customer environments. This effort includes active research for

new and emerging threats. It also includes focused batch hunting that extracts suspicious logs warranting either special review or logs that should be automatically sent to customers

Identity & Access Management (IAM)

Identity & Access Management (IAM) enables the administration and authorization of accesses to specific resources and provides a unified view into security policies across entire organizations with built-in auditing.

Identity Platform

Identity Platform is a customer identity and access management (CIAM) platform delivered by Google Cloud enabling organizations to add identity management and user security to their applications or services.

Key Access Justifications (KAJ)

Key Access Justifications (KAJ) provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at-rest to in-use.

Managed Service for Microsoft Active Directory (AD)

Managed Service for Microsoft Active Directory (AD) is a Google Cloud service running Microsoft AD that enables customers to deploy, configure and manage cloud-based AD-dependent workloads and applications. It is a fully managed service that is highly available, applies network firewall rules, and keeps AD servers updated with Operating System patches.

Privileged Access Manager

Privileged Access Manager (PAM) allows customers to control just-in-time temporary privilege elevation for select principals, and to view audit logs afterwards to find out who had access to what and when.

Organization Policy

Organization Policy provides customizable security guardrails to centrally enforce resource configuration compliance across resource hierarchies.

reCAPTCHA Enterprise

reCAPTCHA Enterprise helps detect fraudulent activity on websites using risk analysis techniques to distinguish between humans and bots.

Resource Manager API

Resource Manager API allows users to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects) to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization enables users to manage common aspects of resources such as access control and configuration settings.

Risk Manager

Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including CIS benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.

SecLM

SecLM or more specifically, the SecLM Platform (formerly known as Security AI Workbench or SAW) - refers to the API and platform that we've built based on the SecPaLM models. The platform orchestrates reasoning, extensions, retrieval augmented generation (RAG), and other techniques to leverage authoritative security data from sources, like Mandiant Advantage Threat Intelligence (MATI) and VirusTotal, and deliver the highest quality responses to security-related prompts.

Secret Manager

Secret Manager provides a secure method for storing API keys, passwords, certificates, and other sensitive data.

Security Command Center

Security Command Center is a log monitoring and security scanning tool that generates analytics and dashboards to help customers to prevent, detect, and respond to Google Cloud security and data threats.

Sensitive Data Protection (including Cloud Data Loss Prevention)

Sensitive Data Protection is a fully-managed service enabling customers to discover, classify, de-identify, and protect sensitive data, such as personally identifiable information.

VirusTotal

VirusTotal enables organizations to research and hunt for malware, to investigate security incidents, to automate analysis, and to keep user investigations private and secure.

VPC Service Controls

VPC Service Controls provides administrators with the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks.

Web Risk API

Web Risk API is a Google Cloud service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.

Serverless Computing

Cloud Functions

Cloud Functions is a serverless compute solution that runs single-purpose functions in response to GCP events and HTTP calls (webhooks). Cloud Functions can be triggered asynchronously by Cloud Pub/Sub, Cloud Storage, GCP infrastructure events, and Firebase products. Cloud Functions scales automatically to meet request load and the user does not need to manage servers or the runtime environment.

Cloud Functions for Firebase

Cloud Functions for Firebase are developer tools used for development and deployment of Google Cloud Functions. Cloud Functions enable developers to run their own backend code that executes automatically based on HTTP requests and Firebase and Google Cloud Platform events. Developers' functions are stored in Google's cloud and run in a managed Node.js environment.

Cloud Run

Cloud Run (fully managed) is a serverless, managed compute platform that automatically scales stateless HTTP containers, running requests or event-driven stateless workloads. Cloud Run provides the flexibility to run services on a fully managed environment.

Cloud Scheduler

Cloud Scheduler is a fully managed enterprise-grade cron job scheduler. It allows customers to schedule jobs, including batch, big data jobs, cloud infrastructure operations, and more. It also acts as a single interface for managing automation tasks, including retries in case of failure to reduce manual toil and intervention.

Cloud Tasks

Cloud Tasks is a fully managed service that allows customers to manage the execution, dispatch, and delivery of a large number of distributed tasks.

Datastream

Datastream is a serverless and easy-to-use change data capture (CDC) and replication service that allows users to synchronize data streams across heterogeneous databases and applications reliably and with minimal latency. Datastream supports streaming changes to data from Oracle and MySQL databases into Cloud Storage.

Eventarc

Eventarc is a fully managed service for eventing on Google Cloud Platform. Eventarc connects various Google Cloud services together, allowing source services (e.g., Cloud Storage) to emit events that are delivered to target services (e.g., Cloud Run or Cloud Functions).

Workflows

Workflows is a fully managed service for reliably executing sequences of operations across microservices, Google Cloud services, and HTTP-based APIs.

Storage

Backup for GKE

Backup for GKE enables data protection for workloads running in Google Kubernetes Engine clusters.

Cloud Filestore

Cloud Filestore is a service for fully managed Network File System (NFS) file servers for use with applications running on Compute Engine virtual machines (VMs) instances or Google Kubernetes Engine clusters.

Cloud Storage

Cloud Storage is Google Cloud Platform's unified object/blob storage. It is a RESTful service for storing and accessing data on Google Cloud Platform's infrastructure. It combines the simplicity of a consistent API and latency across different storage classes with reliability, scalability, performance and security of Google Cloud Platform.

Cloud Storage for Firebase

Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for Firebase apps. Cloud Storage for Firebase is backed by Cloud Storage, a service for storing and accessing data on Google's infrastructure.

Parallelstore

Parallelstore is a parallel file system for high-performance computing and AI/ML workloads. Built on the Distributed Asynchronous Object Storage (DAOS) architecture, Parallelstore combines a fully distributed metadata and key-value architecture to deliver high-performance throughput and IOPS.

Persistent Disk

Persistent Disk provides a persistent virtual disk for use with Google Compute Engine and Google Kubernetes Engine compute instances. It is available in both SSD (Solid State Drive) and HDD (Hard Disk Drive) variations.

Other

Cloud Billing

Cloud Billing provides methods to programmatically manage billing for projects on the Google Cloud Platform.

Google Earth Engine

Google Earth Engine combines a multi-petabyte catalog of satellite imagery and geospatial datasets with planetary-scale analysis capabilities. Scientists, researchers, and developers can use Earth Engine to detect changes, map trends, and quantify differences on the Earth's surface.

Google Cloud Marketplace

Google Cloud Marketplace offers ready-to-go development stacks, solutions, and services from third-party partners and Google to accelerate development. It enables the deployment of production-grade solutions, obtains direct access to partner support, and receives a single bill for both GCP and third-party services.

Google Cloud Skills Boost

Google Cloud Skills Boost is where you can access Google Cloud’s entire catalog of labs and courses. Customer end users can discover learning paths, build in-demand cloud skills, track your activity progress, and validate your knowledge with badges.

Tables

Tables is a lightweight collaborative database to help organize and automate tasks or processes for small teams and businesses.

Data Centers

The above products are serviced from data centers operated by Google around the world. Below is a list of Google's production data center locations that host the above products and operations for Google Cloud Platform. The scope of this report does not cover Google edge points of presence (PoPs).

North America, South America

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Austin (TX), United States of America**
- Chandler (AZ), United States of America
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Gainesville (VA), United States of America

- Guanajuato, Mexico
- Henderson (NV), United States of America
- Lancaster (OH), United States of America
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Markham, Ontario, Canada
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America*
- Midlothian (3) (TX), United States of America***
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada
- Montreal (2), Quebec, Canada
- New Albany (OH), United States of America
- Omaha (NE), United States of America
- Osasco, Brazil
- Papillion (NE), United States of America
- Phoenix (AZ), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile
- Quilicura (3), Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- San Bernardo, Santiago, Chile
- Santana de Parnaíba, Brazil
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- The Dalles (3) (OR), United States of America**
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada
- Vinhedo, Brazil
- Widows Creek (AL), United States of America

Europe, Middle East, and Africa

- Berlin (1), Germany
- Berlin (2), Germany
- Berlin (3), Germany
- Dammam, Saudi Arabia
- Dammam (2), Saudi Arabia*
- Dammam (3), Saudi Arabia*
- Dalarna, Sweden
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, The Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Frankfurt (9), Hesse, Germany**
- Fredericia, Denmark
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- Johannesburg (1), South Africa
- Johannesburg (2), South Africa
- Johannesburg (3), South Africa
- London (1), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Middenmeer, Noord-Holland, The Netherlands
- Milan (1), Italy
- Milan (2), Italy

- Milan (3), Italy
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland

Asia Pacific

- Changhua, Taiwan
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India
- Delhi (4), India***
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Lok Yang Way, Singapore
- Loyang, Singapore
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia
- Mumbai (1), India

- Mumbai (2), India
- Mumbai (3), India
- Mumbai (4), India
- Mumbai (5), India***
- Osaka (1), Japan
- Osaka (2), Japan
- Seoul (1), South Korea
- Seoul (2), South Korea
- Seoul (3), South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Wenya, Singapore

* Indicates data center is in scope only for the period 1 November 2024 through 31 July 2025

** Indicates data center is in scope only for the period 1 March 2025 through 31 July 2025

*** Indicates data center is in scope only for the period 1 May 2025 through 31 July 2025

Infrastructure

Google Cloud Platform runs in a multi-tenant, distributed environment on synchronized internal system atomic clocks and global positioning systems (GPS). Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For Google Cloud Platform, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Customer data is then stored in large, distributed databases, built on top of this file system.

Data Centers and Redundancy

Google maintains consistent policies and standards across its data centers and for physical security to help protect production servers, network devices and network connections within Google data centers.

Redundant architecture exists such that data is replicated in real-time to at least two (2) geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Google uses monitoring mechanisms that provide details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

Authentication and Access

Strong authentication and access controls are implemented to restrict access to Google Cloud Platform production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) and Secure Sockets Layer (SSL) certificates, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google uses encryption to secure user data in transit between Google production facilities. Access to internal support tools, those used by Google operational staff to maintain and troubleshoot the systems for Google Cloud Platform products is controlled via Access Control Lists (ACLs) thus limiting the use of these tools to only those individuals that have been specifically authorized.

Digital certificates used for machine authentication and data encryption are issued by an internal Google certificate authority. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to the Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication.

Google follows a formal process to grant or revoke personnel access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system which utilizes Secure Shell (SSH) and TLS/SSL certificates help provide secure and flexible access. These mechanisms are designed to grant access rights to systems and data only to authorized users. Additionally, access requests via "on demand" mechanisms are reviewed and approved by an authorized second individual prior to being granted and the event is logged.

Both user and internal access to customer data is restricted through the use of unique user account IDs and via the Google Accounts Bring Your Own Identity (BYOID) system for external users. Access to sensitive systems and applications requires two-factor authentication in the form of a unique user account ID, strong passwords, security keys and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semiannual basis under the direction of the group administrators, and any inappropriate access identified is removed.

Access authorization in Google Cloud Platform products is enforced at all relevant layers of the system. The granting or modification of access rights is based on the user’s job responsibilities or on a need-to-know basis and must be authorized and approved by the user’s functional manager or system owners. Approvals are managed by workflow tools and are logged. Production system access is only granted to individuals who require this level of access to perform necessary tasks. Additionally, all users with access to production systems are required to complete security and privacy training annually. Access to individual production systems via critical access groups is reviewed on a periodic basis by the system owners and inappropriate access is removed for Google personnel who no longer have a business need for such access. Access to all corporate and production resources is automatically removed upon submission of a termination request by

the manager of any departing employee, temporary worker, contractor or vendor, or by the appropriate Human Resources manager.

Change Management

Changes to Google Cloud Platform are delivered as software releases through three (3) pipelines:

- Product functionality change or builds related to the service running in Google's production environment;
- Images, downloads, or software updates made available to customers; and
- Open source code packages maintained in a public source code repository.

Changes including configuration changes, code modifications, and new code creation, follow this change management process. Change Management policies and guidelines, including code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented. Each service has documented release processes that specify the procedures to be used, including definition of the scope of changes to be delivered, source code control, code review, building, testing, and record keeping. Development, testing, and build environments are separated from the production environment through the use of logical security controls.

The change process starts with a developer checking out a copy of source code files from the source code management system to modify them. Once development is complete, the developer initiates applicable testing and code reviews. Once the change has received the appropriate code review, the change can be submitted making it the new head version. Google requires that production code reviewers be independent of the developer assigned to the change and follows Google coding standards, in accordance with their policy. Production code reviews are systematically enforced. Emergency changes to production environments must have a valid justification, and are logged, monitored and reviewed.

If needed, once the code is submitted, it can be used to build packages or binaries. During the build process, code is subject to automated testing, the results of which are monitored by engineers. Successfully built packages or binaries can be migrated to staging or QA environments where they can be subject to additional review. When the approved change is ready for deployment to production, it is deployed in a controlled manner, with monitoring in place to notify engineers of anomalies in the deployment. The process from build to release is aided by several tools that automate tasks, including testing and deployment. Employees at Google have the ability to view changes, however, access to modify code and approve changes is controlled via functionality of internal tools that support the build and release process. Changes to customer facing services that may affect confidentiality, security, privacy, and/or availability are communicated to relevant personnel and impacted customers. In addition, implementations and customizations by end-user customers after source code has been made available by Google in the public repositories are out of scope.

Guidelines are made available internally to govern the installation of software on organization-owned assets. Additionally, tools are utilized to detect deviations from pre-defined Operating

System (OS) configurations on production machines and correct them automatically. This allows for an easy roll out of updates to system files in a consistent manner and helps ensure that machines remain in a known current state.

Data

Google provides controls at each level of data storage, access, and transfer. Google has established training programs for privacy and information security to support data confidentiality. Relevant Google personnel, including employees, temporary workers, vendors and contractors are required to complete these training programs at the time of joining the organization and annually thereafter. All new products and product feature launches that include collection, processing, or sharing of user data are required to go through an internal design review process that defines retention and deletion timelines. This review is performed by legal and privacy teams. In addition to the preventative controls, Google has also established detective measures to investigate and determine the validity of security threats. In the case of an incident there are incident response processes to report and handle events related to topics such as security, availability, and confidentiality. Google establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchange with external parties.

Network Architecture and Management

The Google Cloud Platform system architecture utilizes a fully redundant network infrastructure. Border routers that provide the connection point between Google Cloud Platform and any Internet Service Providers are designed to run in a redundant configuration. Where border routers are in use, firewalls are also implemented to operate in a redundant configuration.

Google has implemented perimeter devices to protect the Google network from external network attacks and configurations of perimeter devices are centrally managed. Google segregates networks based on the types of services, users, and information systems. The network is managed via specialized tools. Google employs automated tools to inventory network devices and machines. Authorized security and network engineers access the network devices (production routers and switches) to monitor, maintain, manage, and secure the network through these tools.

Network monitoring mechanisms are in place to detect and prevent access to the Google network from unauthorized devices. Current and previous versions of each router configuration are maintained. Google has documented procedures and checklists for configuring and installing new servers, routers and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet.

Google has a firewall configuration policy that defines acceptable ports that may be used on a Google firewall. Only authorized services and protocols that meet Google's requirements are permitted access to the network. The firewalls are designed to automatically deny all unauthorized

packets not configured as acceptable. Administrative access to the firewalls is limited to authorized administrative personnel using the Secure Shell (SSH) protocol and two-factor authentication. Changes to network configurations are peer reviewed and approved prior to deployment. Google has implemented automated controls on network devices to identify distributed denial of service (DDOS) attacks. Google has established incident response processes to report and handle such events (see the Incident Management section).

People

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform products to customers. The fundamentals underlying the services provided are the adoption of standardized, repeatable processes; the hiring and development of highly skilled resources; and leading industry practices. Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, confidentiality, and privacy controls.

Google has established company structures and reporting lines and has helped ensure sufficient authorities are available to support compliance activities with regulatory, legal, contractual, and privacy requirements. Formal organizational structures exist and are available to Google personnel, including employees, temporary workers, vendors, and contractors, on the Company's intranet. The intranet provides drill-down functionality for identifying personnel in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Policies are reviewed annually, and other materials derived from policies, like guidelines, frequently asked questions (FAQs), and other related documents are reviewed and updated as needed.

User Entity Responsibilities

Cloud security is a shared responsibility between a cloud service provider and its customers. Google Cloud Platform controls were designed with the assumption that certain controls should be implemented by user entities (or "customers"). These controls are known as user entity responsibilities.

This section describes additional controls that customers should consider implementing to complement the controls of the Google Cloud Platform. The list of customer control considerations presented below do not represent a comprehensive set of all the controls that should be employed by customers. Customers may be required to implement additional administrative or technical controls to meet their business and legal needs.

User Entity Responsibilities	Trust Services Criteria
Customers are responsible for assigning responsibilities for the operation and monitoring of the Google Cloud Platform System.	Common Criteria 1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Cloud Platform System.	Common Criteria 1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
Customers are responsible for providing the appropriate training to end-users on proper use of the Google Cloud Platform System consistent with the Acceptable Use Policies and Terms of Service. Acceptable Use Policies available at (or such URL as Google may provide): • Google Cloud Platform: https://cloud.google.com/terms/aup • Chronicle (Security Product) and Threat Intelligence for Chronicle: https://chronicle.security/legal/service-terms/ https://chronicle.security/legal/acceptable-use-policy/	Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
Customers are responsible for ensuring that end-users are trained on the organizational policies and procedures relevant to the use of the Google Cloud Platform System.	Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
Customers should train administrators and end-users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of the Google Cloud Platform System.	Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
Customers are responsible for training users on the use and disclosure of passwords used to authenticate to the Google Cloud Platform System.	Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
Customers are responsible for considering information security requirements in the deployment, configuration, and modification	Common Criteria 1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

User Entity Responsibilities	Trust Services Criteria
of their instance of the Google Cloud Platform System.	Common Criteria 5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
Customers are responsible for defining, documenting, and making available to users procedures for the operation of their instance of the Google Cloud Platform System.	Common Criteria 2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	Common Criteria 2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
Customers should contact Google if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account, compromise of data, and security events.	Common Criteria 2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.
	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
Customers are responsible for ensuring any application software which they deploy onto the Google Cloud Platform System follows	Common Criteria 4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the

User Entity Responsibilities	Trust Services Criteria
their specific software change management policies and procedures.	components of internal control are present and functioning.
	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for periodically reviewing the configuration of the Google Cloud Platform System to ensure it is consistent with their policies and procedures.	Common Criteria 4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for establishing organizational policies and procedures for the use or integration of third-party services.	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
Customers are responsible for reviewing the information security policies and the security capabilities in the Google Cloud Platform System to determine their applicability and modify their internal controls as appropriate.	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

User Entity Responsibilities	Trust Services Criteria
Customers are responsible for defining and maintaining policies and procedures governing the customer's administration of access to the Google Cloud Platform System.	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
Customers are responsible for establishing documented policies and procedures for the transfer and sharing of information within their organization and with third-party entities.	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
	Privacy Criteria 6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.
	Privacy Criteria 6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.
Customers are responsible for provisioning, maintaining, monitoring and disabling end users' access in accordance with their internal access management policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege

User Entity Responsibilities	Trust Services Criteria
	and segregation of duties, to meet the entity's objectives.
	Privacy Criteria 5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.
Customers are responsible for provisioning service availability, user roles, and sharing permissions within the Google Cloud Platform System consistent with customer organizational policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for implementing secure log-on procedures to access the Google Cloud Platform System consistent with customer access management policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for provisioning, maintaining, and disabling end users' access in accordance with customer access management policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for reviewing users' access rights periodically, consistent with customer organizational policies, to mitigate the risk of inappropriate access.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for enabling and enforcing the use of two-step verification on privileged administrator accounts.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for establishing procedures to allocate the initial password to access the Google Cloud Platform System to end-users when Google password authentication is used.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for configuring GCP Marketplace permissions in Google Cloud Platform consistent with customer's internal policies (GCP Marketplace contains enterprise applications that can be added to a Google Cloud Platform).	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for restricting access to and monitoring the use of Application Programming Interfaces (APIs) available in the Google Cloud Platform System.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for configuring domain settings related to integration with other systems within the customer's environment consistent with customer policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for ensuring that user data is exported and deleted from the Google Cloud Platform System before or within a reasonable amount of time after termination.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for ensuring appropriate physical security controls over all devices that access the Google Cloud Platform System.	Common Criteria 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	Common Criteria 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
Customers are responsible for ensuring any devices that access the Google Cloud Platform System or contain customer data are properly handled, secured, and transported as defined by the products requirements.	Common Criteria 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	Common Criteria 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

User Entity Responsibilities	Trust Services Criteria
Customers are responsible for configuring the Google Cloud Platform System mobile device options consistent with customer policies and procedures.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
Customers are responsible for configuring data storage locations that support their business and operational resiliency requirements.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
Customers are responsible for enabling logging and monitoring functionalities to detect administrator activity, customer support activity, security events, system errors, and data deletions to support customer incident management processes.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Cloud Platform System.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Privacy Criteria 7.1: The entity collects and maintains accurate, up-to-date, complete, and

User Entity Responsibilities	Trust Services Criteria
	relevant personal information to meet the entity's objectives related to privacy.
Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Cloud Platform System.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Privacy Criteria 7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.
Customers are responsible for the deployment, configuration and modification of default security settings for cloud products including virtual machines in accordance with their information security requirements.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for ensuring that individuals creating and/or updating profiles or changing the product configurations are authorized.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for reviewing and testing features, builds, and product releases, including Application Programming Interfaces (APIs), to evaluate their impact prior to deploying into production environments, as applicable.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for configuring test and/or development environments in their instance of the Google Cloud Platform System, as applicable, and restricting access to data in these environments.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for managing and testing configurations that support their business and operational resiliency objectives, and for considering Google Cloud Platform architecture recommendations.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

User Entity Responsibilities	Trust Services Criteria
Customers are responsible for training, testing, and deploying AI models that are used in AI-powered applications.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for implementing any custom code necessary for the deployment of the products, and any code in public repositories for customization of their implementations.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for ensuring they have business recovery and backup procedures over their non-Google managed information systems that access the Google Cloud Platform System.	Common Criteria 9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
	Common Criteria 9.2: The entity assesses and manages risks associated with vendors and business partners.
Customers are responsible for ensuring that administrators do not send unnecessary employee personal data when escalating support requests to service providers, including Google.	Confidentiality Criteria 1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
	Privacy Criteria 4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.
	Privacy Criteria 5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.
Customers are responsible for providing permission or instructions to utilize their data and defining the scope of data for training or fine-tuning AI/ML models.	Confidentiality Criteria 1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
	Privacy Criteria 4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

User Entity Responsibilities	Trust Services Criteria
	Privacy Criteria 5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.

Attachment B - Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Google Cloud Platform System. Commitments to customers are communicated via Terms of Service, Google Cloud Platform Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

System Requirements

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform System products to customers. These internal policies are developed in consideration of legal and regulatory obligations, to define Google's organizational approach and system requirements.

The delivery of these services depends upon the appropriate internal functioning of system requirements defined by Google to meet customer commitments.

The following processes and system requirements function to meet Google's commitments to customers with respect to the terms governing the security and privacy of customer data:

- **Access Security:** Google maintains data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege
- **Change Management:** Google requires standard change management procedures to be applied during the design, development, deployment, and maintenance of Google applications, systems, and services
- **Incident Management:** Google monitors security event logs and alerts to determine the validity of security or privacy threats. Potential threats, including threats related to security and privacy, are escalated to the appropriate team including incident management. Google's dedicated security personnel will promptly investigate and respond to potential and known incidents
- **Data Management:** Google complies with any obligations applicable to it with respect to the processing of Customer Personal Data. Google processes data in accordance with Google Cloud Platform Terms of Service and/or Data Processing Agreements, and complies with applicable regulations
- **Data Security:** Google maintains data security and privacy policies and implements technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Google takes appropriate steps to ensure compliance with the security measures by its employees, contractors and vendors to the extent applicable to their scope of performance

- **Third-Party Risk Management:** Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Google conducts routine inspections of subprocessors to ensure their continued compliance with the agreed upon security and privacy requirements. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from suppliers to comply with these practices

Google Confidental Information

MASTERMIND

CERTIFICATE #
MMIND-24112501

CERTIFICATE OF REGISTRATION

Artificial Intelligence Management System - ISO/IEC 42001:2023

Mastermind Assurance, LLC hereby confirms, as a result of its certification decision according to ISO/IEC 17021-1, that the organization maintains a management system conforming to the requirements of ISO/IEC 42001:2023

Google LLC

Scope

The certificate scope comprises the management system supporting the operations underlying the Vertex AI Platform, AI Platform Training and Prediction, Document AI, Vertex AI Search for Industry, Generative AI on Vertex AI, Gemini for Google Cloud, Cloud Translation API, Speech-to-Text, Text-to-Speech, Gemini for Workspace, and Gemini App (also known as "Gemini") product offerings.

These activities are governed by the implemented controls and service-specific roles, including AI Producer and AI Provider, in accordance with the organizational Statement of Applicability.

Statement of Applicability Version:
November 18, 2024

Authorized By:

David Forman
Chief Executive Officer

ISO 42001 CERTIFIED ARTIFICIAL INTELLIGENCE

IAS ACCREDITED Management Systems Certification Body
MSCB-356

Issuance Date
November 25, 2024

Original Registration Date
November 25, 2024

Expiration Date
November 24, 2027

Certification pertains exclusively to the specified management system and does not broaden the scope of the conformity decision to encompass proprietary products, processes, or services. References to sources of controls sets applied within the Statement of Applicability do not represent certification thereof. A unique identification code incorporated in this certificate, along with the certification body's seal and the accreditation mark, must not be cited in advertisements or promotional materials tailored to specific products or services. The certified organization agrees to continue to comply with the obligations detailed within its certificate agreement and in conformity with the underlying schemes comprising the certification criteria. Mastermind Assurance, LLC maintains its operations at 44 Milton Avenue #1026, Alpharetta, Georgia, 30009, United States. This certificate of registration is issued without any explicit or implicit representations or warranties, including but not limited to assurances regarding the qualification or suitability of any particular product.

Google Confidental Information

Site Address	Site Activities
111 8th Avenue New York, NY 10011 United States	• Operational control • Policy maintenance • Cloud engineering services • Customer success and sales • System development lifecycle • Application security • Employee onboarding • Endpoint monitoring • Product and quality management • Sales operations and contracting

bernard@botmaker.io

Docusign Envelope ID: E9DF4AC3-06DB-4BFF-A6DF-8E3A794C6C6B

Accredited Certification Body SAC
MTCS-2018-07

Certificate

Certificate number: 2018-014

Certified by EY CertifyPoint since: July 10, 2018

Based on certification examination in conformity with defined requirements in Multi-Tier Cloud Security – SS 584:2020 as defined and implemented by

Google LLC*

located in Mountain View, California, United States of America is compliant with the Level 3 requirements as stated in the standard:

Multi-Tier Cloud Security – SS 584:2020

Issue date of certificate: June 26, 2024
Re-issue date of certificate: July 25, 2025
Expiration date of certificate: July 9, 2027
Last certification cycle expiration date: July 9, 2024

EY CertifyPoint will, according to the certification agreement dated May 23, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

**The certification is applicable for the assets, services and locations as described in the scoping section at the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, version 1.4, dated May 28, 2025.*

DocuSigned by:
Jatin Sehgal
3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V, located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Docusign Envelope ID: E9DF4AC3-06DB-4BFF-A6DF-8E3A794C6C6B

Google LLC

Scope for certificate 2018-014

The scope refers to level 3 of Multi-Tier Cloud Security System of Google LLC, located in Mountain View, California, United States of America, supporting the provision of Google Cloud using Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) models and implemented in the following product area, its offering(s) and locations as listed below, along with the data contained or collected by those offering(s).

Google Cloud Platform:

- Access Approval
- Access Context Manager
- Access Transparency
- Advanced API Security
- Agent Assist
- AI Platform Deep Learning Container
- AlloyDB
- Anti-Money Laundering AI
- API Gateway
- Apigee
- App Engine
- Application Integration
- Artifact Analysis
- Artifact Registry
- Assured Workloads
- AutoML Tables
- AutoML Translation
- Backup for GKE
- Batch
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- Certificate Authority Service
- Certificate Manager
- Chrome Enterprise Premium
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Billing
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Console
- Cloud Console App
- Cloud Data Fusion
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud External Key Manager (Cloud EKM)
- Cloud Filestore
- Cloud Functions
- Cloud Functions for Firebase
- Cloud Healthcare
- Cloud HSM
- Cloud IDS (Cloud Intrusion Detection System)
- Cloud Interconnect
- Cloud Key Management Service
- Cloud Life Sciences
- Cloud Load Balancing
- Cloud Logging
- Cloud Monitoring
- Cloud NAT (Network Address Translation)
- Cloud Natural Language API
- Cloud NGFW
- Cloud Org Policy
- Cloud Profiler
- Cloud Router
- Cloud Run
- Cloud Scheduler
- Cloud Service Mesh
- Cloud Shell
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speaker ID
- Cloud SQL
- Cloud Storage
- Cloud Storage for Firebase

Docusign Envelope ID: E9DF4AC3-06DB-4BFF-A6DF-8E3A794C6C6B

Google LLC

Scope for certificate 2018-014

Google Cloud Platform (continued):

- Cloud Tasks
- Cloud Trace
- Cloud Translation
- Cloud Vision
- Cloud VPN
- Cloud Workstations
- Compute Engine
- Connect
- Container Registry
- Conversational AI
- Conversational Insights
- Data Catalog
- Database Migration Service
- Dataflow
- Dataform
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- Datastream
- Dialogflow
- Document AI
- Document AI Warehouse
- Eventarc
- Firebase App Check
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Food Ordering AI Agent
- Gemini for Google Cloud
- Generative AI on Vertex AI
- GKE Enterprise Config Management
- GKE Identity Service
- Google Cloud Armor
- Google Cloud Backup and DR
- Google Cloud Contact Center as a Service (CCaaS)
- Google Cloud Deploy
- Google Cloud Identity-Aware Proxy
- Google Cloud Marketplace
- Google Cloud SDK
- Google Cloud Skills Boost
- Google Earth Engine
- Google Kubernetes Engine
- Google Public DNS
- Google Security Operations (SIEM)
- Google Security Operations (SOAR)
- Google Threat Intelligence
- GTI for Google Security Operations
- Healthcare Data Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- Infrastructure Manager
- Integration Connectors
- Key Access Justifications (KAJ)
- Knative serving
- Looker (Google Cloud core)
- Looker Studio
- Managed Service for Apache Kafka
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Migrate to Virtual Machines
- Migration Center
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- Parallelstore
- Persistent Disk
- Personalized Service Health
- Privileged Access Manager
- Pub/Sub
- Ray on Vertex
- reCAPTCHA Enterprise
- Recommendations AI
- Recommender
- Resource Manager API
- Retail Search

This scope is only valid in connection with certificate 2018-014.

Docusign Envelope ID: E9DF4AC3-06DB-4BFF-A6DF-8E3A794C6C6B

Google LLC

Scope for certificate 2018-014

Google Cloud Platform (continued):

- Risk Manager
- SecLM
- Secret Manager
- Secure Source Manager
- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- Service Directory
- Service Infrastructure
- Service Mesh
- Spectrum Access System
- Speech-to-Text
- Storage Transfer Service
- Tables
- Talent Solution
- Text-to-Speech
- Traffic Director
- Transcoder API
- Transfer Appliance
- Vertex AI Colab Enterprise
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Vertex AI Workbench Instances
- Video Intelligence API
- Virtual Private Cloud
- VirusTotal
- VPC Service Controls
- Web Risk API
- Workflows
- Workload Manager

Google Cloud Platform (GCP) Bare Metal (Rack) HSM:

- Bare Metal HSM
- Bare Metal Rack HSM

Google Cloud Platform (GCP) Cloud Software:

- Binary Authorization - Software
- Cloud Monitoring - Software
- Connect - Software
- GKE Enterprise Config Management - Software
- GKE Identity Service - Software
- GKE on AWS
- GKE on Azure
- Google Distributed Cloud Hosted (GDCH) - Software
- Google Distributed Cloud Virtual (GDCV) for Bare Metal
- Google Distributed Cloud Virtual (GDCV) for VMware
- Knative serving - Software
- Migrate to Containers
- Network Gateway for Google Distributed Cloud
- Service Mesh - Software
- Speech-to-Text On-Prem
- Telecom Subscriber Insights

GCP Cloud Edge:

- Google Distributed Cloud connected
- Media CDN

Google Cloud Platform Multi-Cloud Services:

- BigQuery Omni

This scope is only valid in connection with certificate 2018-014.

Docusign Envelope ID: E9DF4AC3-06DB-4BFF-A6DF-8E3A794C6C6B

Google LLC

Scope for certificate 2018-014

Google Cloud NetApp Volumes (GCNV):

- Google Cloud NetApp Volumes

Google Cloud VMware Engine (GCVE):

- Google Cloud VMware Engine

The following locations are in scope:

Data Centers:

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Austin (TX), United States of America
- Berlin (1), Germany
- Berlin (2), Germany
- Berlin (3), Germany
- Chandler (AZ), United States of America
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Dalarna, Sweden
- Dammam, Saudi Arabia
- Dammam (2), Saudi Arabia
- Dammam (3), Saudi Arabia
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Frankfurt (9), Hesse, Germany
- Fredericia, Denmark
- Gainesville (VA), United States of America
- Ghlin, Hainaut, Belgium
- Guanajuato, Mexico
- Hamina, Finland
- Henderson (NV), United States of America
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia
- Johannesburg (1), South Africa
- Johannesburg (2), South Africa

Docusign Envelope ID: E9DF4AC3-06DB-4BFF-A6DF-8E3A794C6C6B

Google LLC

Scope for certificate 2018-014

Data Centers (continued):

- Johannesburg (3), South Africa
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Las Vegas (NV), United States of America
- Lancaster (OH), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Lok Yang Way, Singapore
- London (1), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Loyang, Singapore
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Markham, Ontario, Canada
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia
- Middenmeer, Noord-Holland, the Netherlands
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada
- Montreal (2), Quebec, Canada
- Mumbai (1), India
- Mumbai (2), India
- Mumbai (3), India
- Mumbai (4), India
- New Albany (OH), United States of America
- Omaha (NE), United States of America
- Osaka (1), Japan
- Osaka (2), Japan
- Osasco, Brazil
- Papillion (NE), United States of America
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Phoenix (AZ), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile
- Quilicura (3), Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- San Bernardo, Santiago, Chile
- Santana de Parnaíba, Brazil
- Seoul (1), South Korea
- Seoul (2), South Korea
- Seoul (3), South Korea
- Sydney (1), NSW, Australia

Docusign Envelope ID: E9DF4AC3-06DB-4BFF-A6DF-8E3A794C6C6B

Google LLC

Scope for certificate 2018-014

Data Centers (continued):

- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- The Dalles (3) (OR), United States of America
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Vinhedo, Brazil
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Wenya, Singapore
- Widows Creek (AL), United States of America
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland

Google Confidental Information

bernard@botmaker.io

Informe de Auditoría del ENS de los sistemas de información que dan soporte a los servicios Google Cloud Platform de Google.

Google, LLC

14/10/2019

Documento de uso interno

BDO

Google Confidental Information

Google, LLC

INFORME DE AUDITORÍA DEL ESQUEMA NACIONAL DE SEGURIDAD ESPAÑOL DE LOS SISTEMAS QUE SOPORTAN LOS SERVICIOS GOOGLE CLOUD PLATFORM DE GOOGLE

(Basado en el Real Decreto 3/2010, de 8 de enero)

14 de octubre de 2019

CONTENIDO

1. INFORME DE AUDITORÍA 2
1.1 Introducción 2
1.2 Objetivo 2
1.3 Alcance 3
1.4 Equipo Auditor 9
1.5 Metodología 9
1.6 Conclusiones 11
2. RESUMEN DE LAS MEDIDAS DE SEGURIDAD 13

bernard@botmaker.io

Google Confidental Information

Rafael Calvo, 18
28010 Madrid
España
www.bdo.es

Google, LLC

INFORME DE AUDITORÍA DEL ESQUEMA NACIONAL DE SEGURIDAD ESPAÑOL DE LOS SERVICIOS DE GOOGLE GOOGLE CLOUD PLATFORM

(Basado en el Real Decreto 3/2010, de 8 de enero)

14 de octubre de 2019

1. INFORME DE AUDITORÍA

1.1. INTRODUCCIÓN

De acuerdo con los términos de nuestra propuesta de servicios profesionales, les presentamos nuestro informe de auditoría del Esquema Nacional de Seguridad, de categoría Alta de los sistemas que soportan los servicios GCP de Google, en cumplimiento del artículo 34 y de acuerdo con lo previsto en el anexo III del Real Decreto 3/2010, de 8 de enero.

Este informe de auditoría ha sido preparado para uso exclusivo de Google, LLC, situado en 1600 Amphitheatre Pkwy, Mountain View, CA 94043, (en adelante Google o la Organización), en el contexto de la revisión de cumplimiento de los requerimientos del Esquema Nacional de Seguridad a categoría Alta, por lo que no deberá ser utilizado para fines distintos al descrito a continuación ni ser distribuido a terceros, salvo requerimiento de la autoridad competente.

1.2. OBJETIVO

Para dar cumplimiento a la normativa vigente, y de conformidad con el artículo 34 y con el Anexo III del RD 3/2010, y su modificación mediante el Real Decreto 951/2015, de 23 de octubre, hemos procedido, a solicitud de Google, a revisar el cumplimiento de los requisitos a categoría Alta establecidos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en los capítulos II y III y en los Anexos I y II.

Nuestra responsabilidad es la emisión de un informe que exprese un dictamen sobre la adecuación de los sistemas que dan soporte a los servicios GCP de Google a las medidas y controles definidos de categoría Alta en el Esquema Nacional de Seguridad, identificar sus deficiencias. Adicionalmente, nuestro informe a categoría Alta incluye los datos, hechos y observaciones en que se basan los dictámenes alcanzados.

Adicionalmente, nuestro informe incluye los datos, hechos y observaciones en los que se basan las conclusiones a las que se ha llegado. Las conclusiones de este informe han sido compartidas con los miembros pertinentes de la dirección.

bernardobotmaker.io

Google Confidental Information

1.3. ALCANCE

Google Cloud Platform (GCP) es un servicio de software empresarial de pago por uso, proporcionado y alojado por Google.

Este servicio de suscripción en la nube proporciona las herramientas para crear, probar e implantar aplicaciones en la infraestructura altamente escalable de Google para las soluciones web, móviles y backend de los clientes.

Todos los clientes reciben un conjunto estándar de funciones para los servicios a los que se suscriben, y los servicios se alojan en un entorno compartido y multi-inquilino.

El alcance de la auditoría incluye los elementos e infraestructura que soportan los siguientes servicios GCP de Google:

Access Transparency
El servicio transparencia de acceso proporciona registros de las acciones tomadas por el personal de Google cuando accede a los datos del cliente incluyendo datos sobre: acciones del equipo de asistencia que haya solicitado por teléfono, investigaciones de ingeniería de nivel bajo de tus solicitudes de asistencia o algunas otras investigaciones hechas por motivos comerciales válidos, como recuperarse de un corte de luz.

AI Platform Training and Prediction
AI Platform Training and Prediction es un servicio gestionado que permite a los usuarios crear fácilmente modelos de aprendizaje de máquinas con marcos de trabajo populares como TensorFlow, XGBoost y Sciki, que proporcionan servicios escalables de formación y predicción que funcionan con grandes conjuntos de datos.

App Engine
App Engine permite la creación y el alojamiento de aplicaciones web en los mismos sistemas que las aplicaciones de Google. App Engine ofrece un rápido desarrollo e implementación. No hay necesidad de administrar servidores u otros componentes de infraestructura de bajo nivel. El escalado y el parcheo de software son manejados por App Engine en nombre del usuario. App Engine también ofrece la posibilidad de crear VMs gestionadas. Además, se pueden crear APIs de cliente para aplicaciones de App Engine mediante Google Cloud Endpoints.

BigQuery
BigQuery es un servicio de análisis de datos totalmente gestionado que ofrece almacenamiento de datos escalable, hasta cientos de terabytes, la capacidad de realizar consultas ad hoc en conjuntos de datos de varios terabytes y la capacidad de compartir información a través de la Web.
BigQuery Data Transfer Service

Cloud Armor
Cloud Armor proporciona configuraciones de control de acceso y defensas a escala contra aplicaciones y ataques multi-vectoriales.

Cloud AutoML Natural Language
AutoML Natural Language permite la categorización del texto de entrada en sus propias etiquetas personalizadas (clasificación supervisada). Los modelos pueden ser específicos para un dominio o caso de uso.

Cloud AutoML Translation
Cloud AutoML Translation permite la formación de modelos personalizados con una experiencia limitada en el aprendizaje automático, de modo que las consultas de traducción devuelven resultados específicos para su dominio. Después de cargar los pares de idiomas traducidos, AutoML Translation capacitará e implementará un modelo que pueda escalarse según sea necesario para satisfacer las demandas de producción. AutoML Translation ofrece la posibilidad de crear un modelo listo para la producción en poco tiempo.

Cloud AutoML Vision
Cloud AutoML Vision permite la formación de modelos personalizados para clasificar las imágenes según las etiquetas definidas. Después de subir y etiquetar las imágenes, Cloud AutoML Vision capacitará a un modelo y gestionará la implementación para adaptarse a las demandas. Cloud AutoML Vision ofrece una alta precisión de modelo y un tiempo rápido para crear un modelo listo para la producción. También soporta modelos para detectar objetos en imágenes y descargar modelos de sólo clasificación para su uso en dispositivos de borde.

Google Confidental Information

Cloud Bigtable
Cloud Bigtable es un servicio de base de datos NoSQL de baja latencia, totalmente gestionado y altamente escalable. Está diseñado para la retención y el procesamiento de datos desde gigabytes hasta petabytes de tamaño.

Cloud Billing API
La API de facturación en la nube proporciona métodos para gestionar de forma programada la facturación de proyectos en Google Cloud Platform.

Cloud Build
Cloud Build permite la creación de imágenes de contenedores a partir del código fuente de la aplicación ubicado en Google Cloud Storage o en un servicio de terceros (por ejemplo, Github, Bitbucket). Las imágenes de contenedores creadas pueden almacenarse en Container Registry e implementarse en Container Engine, Compute Engine, App Engine Flexible Environment u otros servicios para ejecutar aplicaciones desde contenedores Docker.

Cloud CDN
Cloud CDN utiliza los puntos de presencia periféricos distribuidos de Google para almacenar en caché contenido equilibrado de carga HTTP(S).

Cloud Console
Cloud Console es una interfaz basada en web que se utiliza para crear, modificar y gestionar servicios y recursos en la plataforma Google Cloud. Los servicios Cloud pueden adquirirse, configurarse y ejecutarse desde la Cloud Console.

Cloud Console Mobile App
Cloud Console Mobile App es una aplicación móvil nativa que proporciona monitorización, alertas y la capacidad de realizar acciones sobre los recursos.

Cloud Dataflow
Cloud Dataflow es un servicio totalmente gestionado para el procesamiento de datos en paralelo y coherente. Utiliza Apache Beam Software Development Kits (SDKs) con primitivas componibles para construir tuberías de procesamiento de datos para procesamiento por lotes o continuo. Este servicio gestiona el ciclo de vida de los recursos del motor de cálculo para los canales de procesamiento y proporciona una supervisión para entender el estado de los canales.

Cloud Datalab
Cloud Datalab es una herramienta interactiva para la exploración, transformación, análisis y visualización de datos en la plataforma Google Cloud. Proporciona servicios analíticos y de almacenamiento para analizar datos en la plataforma.

Cloud Dataproc
Cloud Dataproc es un servicio gestionado para el procesamiento distribuido de datos. Proporciona herramientas de gestión, integración y desarrollo para desplegar y utilizar Apache Hadoop, Apache Spark, y otras herramientas de procesamiento de datos de código abierto relacionadas. Con Cloud Dataproc, los clústeres pueden crearse y eliminarse bajo demanda y dimensionarse para adaptarse a cualquier carga de trabajo disponible.

Cloud Datastore
Cloud Datastore es una base de datos NoSQL altamente escalable para aplicaciones móviles y web. Proporciona capacidades de consulta, transiciones atómicas, índices y escalas automáticas hacia arriba y hacia abajo en respuesta a la carga.

Cloud Deployment Manager
Deployment Manager es un servicio de gestión de infraestructuras que automatiza la creación y gestión de recursos de Google Cloud Platform.

Cloud DNS
Cloud DNS es un servicio de sistema de nombres de dominio totalmente gestionado que opera una red geográficamente diversa de servidores de nombres autorizados de alta disponibilidad. Cloud DNS proporciona un servicio para publicar y gestionar registros DNS para aplicaciones y servicios.

Cloud Endpoints
Google Cloud Endpoints es una herramienta que proporciona servicios para desarrollar, implementar, proteger y supervisar las API que se ejecutan en la plataforma Google Cloud.

bernardo@otmaker.io

Google Confidental Information

Cloud Filestore
Cloud Filestore es un servicio para servidores de archivos NFS totalmente gestionados para su uso con aplicaciones que se ejecutan en máquinas virtuales (VMs) o clusters de Google Kubernetes Engine.

Cloud Firestore
Cloud Firestore es una base de datos documental NoSQL totalmente administrada, escalable y sin servidor para el desarrollo móvil, web y de servidores. Proporciona capacidades de consulta, fuerte consistencia, sincronización en vivo y soporte offline. También proporciona integraciones tanto con Firebase como con Google Cloud Platform (GCP).

Cloud Functions
Cloud Functions es una solución informática sin servidor que ejecuta funciones de propósito único en respuesta a eventos GCP y llamadas HTTP (webhooks). Las funciones Cloud pueden ser activadas asincrónicamente por Cloud Pub/Sub, Cloud Storage, GCP en eventos de infraestructura y productos Firebase. Cloud Functions se adapta automáticamente para satisfacer la carga de solicitudes y el usuario no necesita administrar servidores ni el entorno de tiempo de ejecución.

Cloud Healthcare
Cloud Healthcare proporciona servicios gestionados y una API para almacenar, procesar, gestionar y recuperar datos sanitarios en una variedad de formatos estándar del sector.

Cloud HSM
Cloud HSM es un servicio de Módulo de seguridad de hardware (HSM) alojado en la nube para alojar claves de cifrado y realizar operaciones criptográficas.

Cloud Identity & Access Management
Cloud Identity and Access Management (IAM) permite la administración y autorización de accesos a recursos específicos, y proporciona una visión unificada de las políticas de seguridad en toda la organización con auditoría incorporada.

Cloud Identity-Aware Proxy
Cloud Identity-Aware Proxy (Cloud IAP) es una herramienta que ayuda a controlar el acceso a las aplicaciones que se ejecutan en Google Cloud Platform en función de la identidad y la pertenencia a un grupo.

Cloud Interconnect
Cloud Interconnect ofrece conexiones de nivel empresarial a Google Cloud Platform. Esta solución proporciona una conexión directa entre las redes locales y GCP Virtual Private Cloud.

Cloud IoT Core
Cloud IoT Core es un servicio totalmente gestionado que conecta, gestiona e introduce datos de dispositivos conectados a Internet de forma segura. Permite la utilización de otros servicios de Google Cloud Platform para recopilar, procesar y analizar datos de IoT.

Cloud Key Management Service
Cloud Key Management Service (KMS) es un servicio de gestión de claves alojado en la nube que gestiona el cifrado de los servicios en la nube. Permite la generación, uso, rotación y destrucción de claves de cifrado.

Cloud Load Balancing
El equilibrio de carga en la nube es un servicio distribuido, definido por software y gestionado para todo el tráfico (HTTP(S), TCP/SSL y UDP) hacia los recursos informáticos. El equilibrio de carga en la nube responde rápidamente a los cambios en el tráfico, la red, el estado del backend y otras condiciones relacionadas.

Cloud Memorystore
Cloud Memorystore para Redis proporciona un servicio de almacenamiento de datos en memoria totalmente gestionado para GCP. Cloud Memorystore se puede utilizar para crear cachés de aplicaciones que proporcionan acceso a datos de baja latencia. Cloud Memorystore es compatible con el protocolo Redis, permitiendo una migración sin problemas y sin cambios de código.

Cloud Natural Language API
Cloud Natural Language proporciona un entendimiento del lenguaje natural como una API fácil de usar. Dado un bloque de texto, esta API permite encontrar entidades, analizar sentimientos (positivos o negativos), analizar sintaxis (incluyendo partes del habla y árboles de dependencia) y categorizar el contenido en una taxonomía rica. La API se puede llamar pasando el contenido directamente o haciendo referencia a un documento en Google Cloud Storage.

bernard@botmaker.co

Google Confidental Information

Cloud Pub/Sub
Cloud Pub/Sub proporciona mensajería asíncrona, fiable y de muchos a muchos entre aplicaciones. Las aplicaciones editoriales pueden enviar mensajes a un "tema", mientras que otras aplicaciones pueden suscribirse a ese tema para recibir los mensajes. Al desacoplar los remitentes y los receptores, Google Cloud Pub/Sub permite la comunicación entre aplicaciones independientes.

Cloud Resource Manager
Cloud Resource Manager permite a los usuarios gestionar de forma programática los recursos de Google Cloud Platform (como organizaciones y proyectos) para agrupar y organizar jerárquicamente otros recursos de Google Cloud Platform. Esta organización jerárquica permite a los usuarios gestionar aspectos comunes de los recursos como el control de acceso y los ajustes de configuración.

Cloud Router
Cloud Router de Google permite la actualización dinámica de las rutas del protocolo BGP (Border Gateway Protocol) entre una red VPC y una red externa, normalmente una red local.

Cloud SDK
Cloud SDK es un conjunto de herramientas de línea de comandos para la plataforma Google Cloud Platform que pueden ejecutarse de forma interactiva o en scripts automatizados. Estas herramientas se pueden utilizar para gestionar los productos compatibles con Google Cloud Platform, como las máquinas virtuales de Compute Engine, los clústeres de Kubernetes, las configuraciones de red y de cortafuegos, y el almacenamiento en disco.

Cloud Security Scanner
Cloud Security Scanner es un escáner de seguridad de aplicaciones web para Google App Engine. Proporciona la capacidad de comprobar un subconjunto de vulnerabilidades comunes de las aplicaciones web en los sitios web creados en App Engine.

Cloud Shell
Cloud Shell proporciona acceso en línea de comandos a los recursos de Google Cloud Platform a través de un shell de Linux en el navegador respaldado por una máquina virtual de Linux temporal en la nube. Permite gestionar proyectos y recursos sin necesidad de instalar herramientas adicionales en los sistemas y viene equipado y configurado con herramientas comunes para desarrolladores como editores de texto, un cliente MySql y kubernetes.

Cloud Source Repositories
Cloud Source Repositories proporciona control de versiones de Git para soportar el desarrollo colaborativo de cualquier aplicación o servicio, así como un navegador de origen que puede ser usado para navegar por el contenido de los repositorios y ver archivos individuales desde la Cloud Console. Los repositorios de código fuente en nube y las herramientas relacionadas (por ejemplo, Stackdriver Debugger) se pueden utilizar para ver la información de depuración junto con el código durante el tiempo de ejecución de la aplicación.

Cloud Spanner
Cloud Spanner es un servicio de base de datos relacional, escalable y totalmente gestionado. Está diseñado para proporcionar una base de datos escalable de procesamiento de transacciones en línea (OLTP) con alta disponibilidad y transacciones ACID (Atomicidad, Consistencia, Aislamiento, Durabilidad) con replicación sincrónica de datos entre regiones.

Cloud Speech-to-Text
Cloud Speech-to-Text permite convertir audio a texto mediante la aplicación de modelos de red neuronal en una API. La API puede reconocer más de 80 idiomas y variantes. Los usuarios pueden transcribir el texto de los usuarios dictando al micrófono de una aplicación, habilitar el comando y control a través de la voz, o transcribir archivos de audio, entre muchos otros casos de uso. La API puede recibir audio en flujo continuo o una URL a audio almacenado en Google Cloud Storage.

Cloud SQL
Cloud SQL es un servicio para crear, configurar y utilizar bases de datos relacionales de terceros gestionadas en Google Cloud Platform. Cloud SQL mantiene, gestiona y administra esas bases de datos.

Cloud Storage
Cloud Storage es el almacenamiento unificado de objetos y bloques de Google Cloud Platform. Es un servicio RESTful para almacenar y acceder a los datos en la infraestructura de Google Cloud Platform. Combina la simplicidad de una API consistente y la latencia en diferentes clases de almacenamiento con la fiabilidad, escalabilidad, rendimiento y seguridad de Google Cloud Platform.

bernard@pdmarket

Google Confidental Information

Cloud Storage Transfer Service
El servicio Cloud Storage Transfer Service permite importar grandes cantidades de datos en línea a Google Cloud Storage. Puede transferir datos desde Amazon Simple Storage Service (Amazon S3) y otras ubicaciones HTTP/HTTTPS, así como datos entre cubos de Google Cloud Storage.

Cloud Talent Solution (Job Search)
Cloud Talent Solution ofrece acceso al aprendizaje automático de Google, lo que permite que los sitios de empleo, las bolsas de trabajo, los ATS, las agencias de empleo y otras plataformas tecnológicas de contratación de personal mejoren la experiencia de adquisición de talento.

Cloud Text-to-Speech
Google Cloud Text-to-Speech sintetiza el sonido natural del habla con 30 voces, disponibles en varios idiomas y variantes para ofrecer audio de alta fidelidad, creando interacciones realistas en muchas aplicaciones y dispositivos.

Cloud Translation
Cloud Translation traduce automáticamente el texto de un idioma a otro (por ejemplo, del francés al inglés). La API se utiliza para traducir sistemáticamente texto en páginas web o aplicaciones.

Cloud Video Intelligence
Cloud Video Intelligence API hace que los vídeos se puedan buscar y descubrir mediante la extracción de metadatos a través de una API REST. Anotan los vídeos almacenados en Google Cloud Storage y ayudan a identificar las entidades sustantivas clave de un vídeo y cuándo se producen en él.

Cloud Vision
Cloud Vision permite comprensión del contenido de la imagen mediante la encapsulación de modelos de aprendizaje de la máquina en una API de REST. Clasifica las imágenes en miles de categorías, detecta objetos y rostros individuales dentro de las imágenes, y encuentra y lee las palabras impresas contenidas en las imágenes. Puede ser aplicado para construir metadatos en catálogos de imágenes, moderar contenido ofensivo, o permitir nuevos escenarios de marketing a través del análisis de sentimiento de imagen. También puede analizar las imágenes cargadas en la solicitud e integrarse con el almacenamiento de imágenes en Google Cloud Storage.

Cloud VPN
La VPN en nube proporciona conexiones entre redes locales u otras redes externas a las Nubes Privadas Virtuales en GCP a través de una conexión IPsec o se puede utilizar para conectar dos gateways VPN gestionados por Google.

Compute Engine
Compute Engine ofrece capacidades de computación de máquinas virtuales escalables y flexibles en la nube. Con máquinas virtuales que pueden arrancar en minutos, ofrece muchas configuraciones, incluyendo tipos de máquinas personalizadas que pueden optimizarse para casos de uso específicos, así como soporte para GPUs, TPUs y SSDs locales.

Container Registry
Container Registry es un sistema privado de almacenamiento de imágenes Docker en Google Cloud Platform.

Data Loss Prevention
Cloud Data Loss Prevention (DLP) permite clasificar, redactar y analizar el contenido sensible o identificado personalmente en texto, imágenes y activos de nube.

Dialogflow Enterprise Edition
Dialogflow es una suite de desarrollo para aplicaciones conversacionales de voz y texto, incluyendo chatbots. Dialogflow es multiplataforma y puede conectarse a aplicaciones (en la web, Android, iOS y IoT) o a plataformas existentes (por ejemplo, Acciones en Google, Facebook Messenger, Slack).

Cloud Life Sciences Service
Cloud Life Sciences Service proporciona una interfaz de programación de aplicaciones (API) para almacenar, procesar, inspeccionar y compartir las lecturas de secuencias de ADN, las alineaciones basadas en referencias y las llamadas de variantes, utilizando la infraestructura de nube de Google.

Google Service Control
Google Service Control proporciona funcionalidad de plano de control a los servicios gestionados, como el registro, y comprobaciones de estado.

Google Confidental Information

Google Service Management
Google Service Management proporciona métodos para publicar servicios gestionados y gestionar configuraciones de servicios.

Kubernetes Engine
Kubernetes Engine, impulsado por el programador de contenedores de código abierto Kubernetes, ejecuta contenedores en Google Cloud Platform. Kubernetes Engine gestiona el aprovisionamiento y mantenimiento del clúster de máquinas virtuales subyacente, las aplicaciones de escalado y la logística operativa, como el registro, la supervisión y la gestión de la salud del clúster.

Network Service Tiers
Los niveles de servicio de red permiten la selección de diferentes redes (niveles) de calidad para el tráfico saliente a Internet: El nivel estándar utiliza principalmente proveedores de tránsito de terceros, mientras que Premium Tiers aprovecha la red troncal privada y la superficie de interconexión de Google para la salida.

Orbitera
Orbitera proporciona una plataforma que crea mercados para vender soluciones, importar datos de facturación y generar informes y facturas, y crear pruebas de software multi-nube con plazos de entrega definidos.

Persistent Disk
Persistent Disk proporciona un disco virtual persistente para su uso con Google Compute Engine y Google Kubernetes Engine para las instancias de cálculo. Está disponible tanto en versión SSD (Solid State Drive) como en versión HDD (Hard Disk Drive).

Service Consumer Management
Service Consumer Management proporciona utilidades para ayudar a los productores de servicios gestionados a gestionar las relaciones con los consumidores de servicios, incluida la capacidad de crear y gestionar unidades de tenencia.

Stackdriver Debugger
Stackdriver Debugger proporciona la capacidad de inspeccionar la pila de llamadas y las variables de una aplicación de nube en ejecución en tiempo real sin detenerla. Es seguro utilizarlo en pruebas, producción o en cualquier otro entorno de implementación. Se puede utilizar para depurar aplicaciones escritas en cualquier lenguaje de programación.

Stackdriver Error Reporting
Stackdriver Error Reporting cuenta, analiza y agrega los fallos en las aplicaciones. Los datos del accidente se extraen de los registros de aplicaciones en Google Cloud o se comunican a través de la API pública. Los datos recopilados pueden ser inspeccionados a través de la interfaz de usuario o de la API pública y pueden optar por recibir notificaciones sobre la ocurrencia de errores.

Stackdriver Logging
Stackdriver Logging es un servicio totalmente gestionado que proporciona un servicio para almacenar, buscar, analizar, supervisar y alertar sobre los datos de registro y los eventos de la plataforma Google Cloud y los servicios web de Amazon (AWS). La API también permite la ingestión de datos de registro personalizados de cualquier fuente. Stackdriver Logging puede ingerir datos de registro de aplicaciones y sistemas de miles de VMs y analizar los datos de registro en tiempo real. El software relacionado con el Stackdriver Logging (es decir, el agente de registro de código abierto) que puede descargarse e instalarse en máquinas virtuales independientes está fuera del alcance de este informe.

Stackdriver Profiler
Stackdriver Profiler recopila y reporta continuamente información de rendimiento a nivel de fuente de los servicios de producción. Proporciona información clave para determinar qué funciones del código consumen la mayor parte de la memoria y los ciclos de la CPU, de modo que se puede obtener información sobre cómo funciona el código para mejorar el rendimiento y optimizar los recursos informáticos.

Stackdriver Trace
Stackdriver Trace recopila los datos de latencia de las aplicaciones y los muestra en la consola de la plataforma Google Cloud. Analiza automáticamente los datos de rastreo para generar informes de rendimiento exhaustivos que ayudan a identificar y localizar los cuellos de botella de rendimiento.

Virtual Private Cloud (VPC)
Virtual Private Cloud es un conjunto completo de capacidades de red gestionadas que incluye selección de rango de direcciones IP granulares, rutas y cortafuegos.

bmarco@bormaker.com

Google Confidental Information

El alcance de la revisión ha contemplado los elementos necesarios para el desarrollo del sistema que soporta el servicio GCP de Google de acuerdo con la Declaración de Aplicabilidad "ENS GCP SOA 2019".

En base a la declaración de aplicabilidad, los siguientes requisitos no se consideran dentro del alcance al no formar parte del servicio estándar objeto de la revisión:

- Medidas de Protección \ Protección de la información:
  - mp.info.4 – Firma electronica
  - mp.info.5 – Sellos de tiempo

Nota: Los clientes que requieran la implementación de los controles indicados pueden configurar los sistemas para utilizar Servicios adicionales.

1.4. EQUIPO AUDITOR

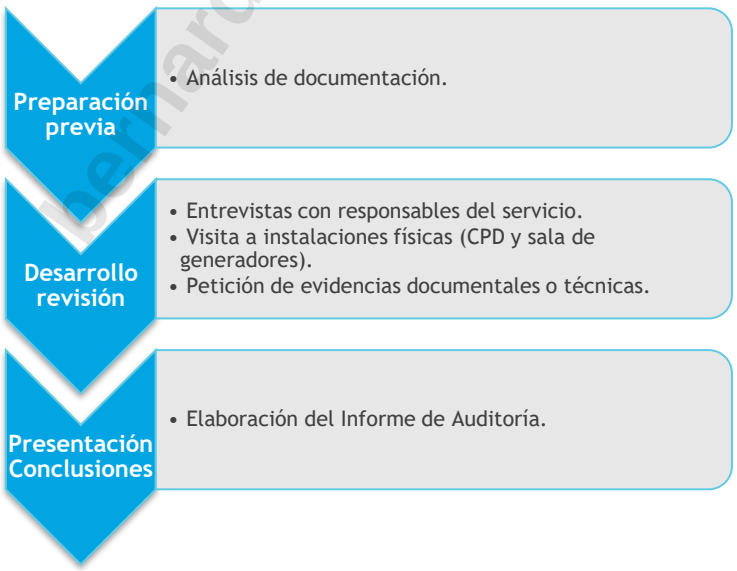
A continuación, se indican los componentes del equipo responsable de la auditoría, así como su función:

EQUIPO AUDITOR	
Juan Manzano	Auditor Jefe
María Riquelme	Auditor

bernard@hotmaker.io

1.5. METODOLOGÍA

La metodología empleada para la realización del presente trabajo, ha consistido en:



- **Preparación previa**: el trabajo de revisión se ha iniciado con un análisis de la documentación facilitada por la Organización, a partir de la que se ha planificado la revisión conjuntamente con los responsables del proyecto de la Organización. Esta fase ha tenido lugar en Junio.

- **Desarrollo de la revisión**: se han validado los procedimientos descritos y se han realizado las pruebas y comprobaciones necesarias para asegurar que se adecuan a la normativa vigente. Esta fase ha tenido lugar entre Julio y Octubre.

Google Confidental Information

- **Entrevistas:** las personas de BDO que han participado en la revisión se han entrevistado con los responsables de Sistema y de Seguridad de Google. Esta fase ha tenido lugar durante los meses de Septiembre y Octubre.

- **Visita a las instalaciones:** se ha realizado una revisión in-situ de los siguientes tipos de dependencias:

  Centro de Procesamiento de Datos: Se ha visitado el centro de procesamiento de Datos de Bélgica que está ubicado en la población de Baudour. Esta visita tuvo lugar el 20 de Junio.

- **Presentación conclusiones:** en la última fase de la metodología, se ha procedido a la validación de la información y se han presentado a la Organización las conclusiones y observaciones derivadas del trabajo realizado.

bernard@botmaker.io

Google Confidental Information

1.6. CONCLUSIONES

Las principales conclusiones obtenidas de nuestro trabajo de revisión de las medidas y controles de seguridad conforme a la categoría Alta del sistema que soporta el servicio Google Cloud Platform de Google son las que se indican a continuación:

a) Google dispone de la preceptiva Política de Seguridad, un marco normativo de seguridad completo y actualizado y del proceso de organización e implantación de la seguridad a través de un sistema de gestión de seguridad de la información documentado, aprobado por su Dirección y certificado. Todo ello permite un proceso de mejora continua de la gestión de la seguridad conforme a lo establecido en los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad.

b) Se definen los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información respectando el principio de "separación de funciones".

c) Existe una adecuada identificación y gestión de riesgos de los sistemas que soportan el servicio GCP, incluyendo la identificación de escenarios de riesgo, el análisis de las consecuencias y su probabilidad, y la evaluación de su aceptabilidad o inaceptabilidad para la Organización, según lo establecido en las medidas aplicables del Anexo II del RD 3/2010.

d) Se cumplen de manera global las medidas de seguridad descritas en el Anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.

e) Las medidas y controles de seguridad de categoría Alta de aquellos aspectos de aplicación para los sistemas de información que soportan el servicio Google Cloud Platform de Google, sus Sistemas de Información e instalaciones de tratamiento de datos cumplen con lo dispuesto en el Real Decreto 3/2010, del 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

f) El dictamen final del informe de auditoría es: **Favorable**

bernard@protmaker.ro

BDO Auditores, S.L.P.



Juan Manzano
Auditor Jefe

Madrid, 14 de Octubre de 2019.

Google Confidental Information

bernard@botmaker.io

RESUMEN DE LAS MEDIDAS DE SEGURIDAD

Informe de Auditoría del ENS de los sistemas de información que soportan los servicios GCP de Google

GCP

Google Confidental Information

2. RESUMEN DE LAS MEDIDAS DE SEGURIDAD

A modo de síntesis, las siguientes tablas indican el grado de cumplimiento en el ENS a categoría Alta en base a los requerimientos normativos establecidos.

MARCO ORGANIZATIVO

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
(org)	1 - Política de Seguridad	✓		
	2 - Normativa de seguridad	✓		
	3 - Procedimientos de seguridad	✓		
	4 - Proceso de autorización	✓		

Leyenda	✓ Cumple	× NC Mayor	× NC Menor	- No aplica
	✓ El servicio de Google permite el cumplimiento; sin embargo, el cumplimiento total depende de la configuración correcta por parte del cliente.			

MARCO OPERACIONAL

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
Planificación (op.pl)	1 - Análisis de Riesgos	✓	✓	✓
	2 - Arquitectura de Seguridad	✓	✓	✓
	3 - Adquisición de nuevos componentes	✓		
	4 - Dimensionamiento / gestión de capacidades		✓	
	5 - Componentes certificados			✓
Control de acceso (op.acc)	1 - Identificación	✓		
	2 - Requisitos de acceso	✓		
	3 - Segregación de funciones y tareas		✓	
	4 - Proceso de gestión de derechos de acceso	✓		
	5 - Mecanismo de autenticación	✓	✓	✓
	6 - Acceso local	✓	✓	✓
	7 - Acceso remoto	✓	✓	
Explotación (op.exp)	1 - Inventario de activos	✓		
	2 - Configuración de seguridad	✓		
	3 - Gestión de la configuración		✓	
	4 - Mantenimiento	✓		
	5 - Gestión de cambios		✓	
	6 - Protección frente a código dañino	✓		
	7 - Gestión de incidentes		✓	
	8 - Registro de la actividad de los usuarios	✓	✓	✓
	9 - Registro de la gestión de incidentes		✓	
	10 - Protección de los registros de actividad			✓
	11 - Protección de claves criptográficas	✓	✓	
Servicios externos (op.ext)	1 - Contratación y acuerdos de nivel de servicio		✓	
	2 - Gestión diaria		✓	
	9 - Medios alternativos			✓

mecanismoplotmaker.io

Google Confidental Information

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
Continuidad del servicio (op.cont)	1 - Análisis del impacto		✓	
	2 - Plan de continuidad			✓
	3 - Pruebas periódicas			✓
Monitorización del sistema (op.mon)	1 - Detección de intrusión		✓	
	2 - Sistema de métricas	✓	✓	✓

Leyenda	✓ Cumple	× NC Mayor	× NC Menor	- No aplica
	✓ El servicio de Google permite el cumplimiento; sin embargo, el cumplimiento total depende de la configuración correcta por parte del cliente.			

MEDIDAS DE PROTECCIÓN

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
Protección de las instalaciones e infraestructuras (mp.if)	1 - Áreas separadas y con control de acceso	✓		
	2 - Identificación de las personas	✓		
	3 - Acondicionamiento de los locales	✓		
	4 - Energía eléctrica	✓	✓	
	5 - Protección frente a incendios	✓		
	6 - Protección frente a inundaciones		✓	
	7 - Registro de entrada y salida de equipamiento	✓		
	9 - Instalaciones alternativas			✓
Gestión del personal (mp.per)	1 - Caracterización del puesto de trabajo		✓	
	2 - Deberes y obligaciones	✓		
	3 - Concienciación	✓		
	4 - Formación	✓		
	9 - Personal alternativo			✓
Protección de los equipos (mp.eq)	1 - Puesto de trabajo despejado	✓	✓	
	2 - Bloqueo de puesto de trabajo		✓	✓
	3 - Protección de equipos portátiles	✓		✓
	9 - Medios alternativos		✓	
Protección de las comunicaciones (mp.com)	1 - Perímetro seguro	✓		✓
	2 - Protección de la confidencialidad		✓	✓
	3 - Protección de la autenticidad y de la integridad	✓	✓	✓
	4 - Segregación de redes			✓
	9 - Medios alternativos			✓
Protección de los soportes de información (mp.si)	1 - Etiquetado	✓		
	2 - Criptografía		✓	✓
	3 - Custodia	✓		
	4 - Transporte	✓		
	5 - Borrado y destrucción	✓	✓	
Protección de las aplicaciones inf. (mp.sw)	1 - Desarrollo de aplicaciones		✓	
	2 - Aceptación y puesta en servicio	✓	✓	✓
Protección de la información (mp.info)	1 - Datos de carácter personal	✓		
	2 - Calificación de la información	✓	✓	
	3 - Cifrado			✓
	4 - Firma electrónica	-	-	-

borrador@makor.io

Google Confidental Information

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
	5 - Sellos de tiempo			-
	6 - Limpieza de documentos	✓		
	9 - Copias de seguridad	✓		
Protección de los servicios (mp.s)	1 - Protección del correo electrónico	✓		
	2 - Protección de servicios y aplicaciones web	✓		✓
	8 - Protección frente a la denegación de servicio		✓	✓
	9 - Medios alternativos			✓

Leyenda	✓ Cumple	× NC Mayor	× NC Menor	- No aplica
	✓ El servicio de Google permite el cumplimiento; sin embargo, el cumplimiento total depende de la configuración correcta por parte del cliente.			

bernard@botmaker.io

Google Confidental Information

PARA MÁS INFORMACIÓN

Juan Manzano

+34 91 436 4190
Juan.manzano@bdo.es

Esta publicación ha sido redactada en términos generales y debe ser contemplada únicamente como una referencia general. Esta publicación no puede utilizarse como base para amparar situaciones específicas y usted no debe actuar, o abstenerse de actuar, de conformidad con la información contenida en este documento sin obtener asesoramiento profesional específico. Póngase en contacto con BDO Auditores, S.L.P. en cualquiera de nuestras oficinas para tratar estos asuntos en el marco de sus circunstancias particulares. BDO Auditores, S.L.P., sus socios y empleados, no aceptan ni asumen cualquier responsabilidad ante cualquier pérdida derivada de cualquier acción realizada o no por cualquier individuo al amparo de la información contenida en esta publicación o ante cualquier decisión basada en ella.

BDO Auditores S.L.P., es una sociedad limitada española, y miembro de BDO International Limited, una compañía limitada por garantía del Reino Unido y forman parte de la red internacional BDO de empresas independientes asociadas.

BDO es la marca comercial utilizada por toda la red BDO y para todas sus firmas miembro.

Copyright © 2017. Todos los derechos reservados. Publicado en España.

bdo.es
bdo.global

Auditoría & Assurance | Advisory | Abogados | Outsourcing

bernard@botnak

Google Confidental Information

sekuro
Trust Tomorrow.

bernard@botmaker.io

IRAP Cloud Security Assessment Report

Google LLC

Version 1.0 | 2/12/2024 | Confidential

DOCUMENT CONTROL

Assessment

ISM version	March 2024
Control classification	PROTECTED
Assessment definition	Hybrid
Deployment model	Public Cloud
Report template version	v5.0 February 2024

Google LLC		
Google	Address	
	Contact Name	Iris Lo
	Contact Email	Irislo@google.com

Prepared by Sekuro	
Address	Level 5/727 George St, Haymarket NSW 2000, Australia
IRAP Assessors	Chris Ekert, Sita Bhat, Prashant Haldankar
Contact Email	chris.ekert@sekuro.io, sita.bhat@sekuro.io, prashant.haldankar@sekuro.io
Assessment Number	Assessment-000375
Sekuro Project Number	P12341
Contributors	Ian Vermeulen

bernard@bootmaker.io

Document History

Version	Date	Section	Amendment	Author
0.1	2/12/2024	All	Initial draft	Chris Ekert
0.2	6/12/2024	All	Quality assurance	Sekuro
0.3	2/2/2024	All	First release	Chris Ekert
0.4	5/2/2025	All	Customer review	Iris Lo
1.0	10/2/2025	All	Final release	Chris Ekert

TABLE OF CONTENTS

1 Executive Summary **5**
1.1 Background 5
1.2 Implementation Summary 6
1.3 Authorisation Considerations 7
2 Introduction **10**
2.1 Cloud Service Provider 10
2.2 Cloud Service Platform 10
2.2.1 Overview 10
2.2.2 Logical Diagram 12
3 Assessment Details **13**
3.1 Methodology 13
3.2 Scope 14
3.2.1 Dependencies and Inheritance 14
3.2.2 CSP Locations 14
3.2.3 Service Regions 14
3.2.4 Cloud Services 15
3.2.5 Exclusions 16
4 CSP Security Fundamentals Assessment **18**
4.1 Security Culture 18
4.1.1 Strengths 18
4.1.2 Weaknesses 19
4.1.3 Response to Cyber Security Incidents 19
4.1.4 Contributions to Cyber Security 19
4.1.5 Cyber Security Guidance 20
4.1.6 Information Security Compliance Certifications 20
4.2 Governance 21
4.2.1 Enterprise Risk Management 21
4.2.2 Personnel Security 21
4.2.3 IT Change Management 22
4.2.4 Data Type Definitions 22
4.2.5 Data Protections 23
4.2.6 Data Deprovisioning and Disposal 24
4.2.7 Supply Chain Risk Management 25
4.2.8 Vulnerability Management 25
4.2.9 Incident Response 26
4.2.10 System Development Lifecycle 27
4.2.11 Support Model 28
4.3 Administrative and Support Environment 30
4.3.1 Administrative and Support System Overview 30
4.3.2 Physical Security 30
4.3.3 Segmentation and Segregation 31
4.3.4 System Hardening 32
4.3.5 Secure Administration 33

bernard@botmaker.io

4.4 CSP's Cloud Protection Environment 35
4.4.1 Network Security 35
4.4.2 Decommissioning Hardware 35
4.4.3 Security Operations and Monitoring 36
4.4.4 Cryptography and Key Management 37
4.4.5 Data Transfers 38
4.4.6 Identity and Access Management 38
4.4.7 Security Automation 39
4.4.8 Continuity and Availability 40
5 Assessment of Cloud Services 41
5.1 Cloud Service Assessment and Consumer Guidance 41
4.1.1 Description 41
5.1.2 Cloud Security Shared Responsibility Model 41
5.1.3 Cloud Service Architecture Diagram 43
5.1.4 Components and Dependencies 43
5.1.5 Inbound and Outbound Interfaces 44
5.1.6 Protection of Data at Rest 44
5.1.7 Data Backup and Restore 45
5.1.8 Data Portability 45
5.1.9 Tenancy Segmentation and Segregation 46
5.1.10 Cloud Service Security Visibility 46
5.1.11 Security Intelligence 47
6 Key Assessment Findings 49
6.1 Cloud Service Provider Implementation 49
6.1.2 Alternate Security Controls 49
6.1.3 Security Controls Not Implemented due to Business Decision 66
6.1.4 Ineffective Security Controls 67
6.1.5 No Visibility Security Controls 71
APPENDIX A Cloud Controls Matrix 73
APPENDIX B Addendums 74

nerd@hotmaker.io

1 Executive Summary

1.1 Background

Google LLC (herein, "Google)" is a multinational technology company specialising in internet-related services and products. Founded in 1998 by Larry Page and Sergey Brin, Google initially focused on developing a powerful search engine and has quickly expanded into a range of technology sectors, including online advertising, cloud computing, software, and hardware. Google's mission is to "organize the world's information and make it universally accessible and useful.[1]"

In addition to its flagship search engine, Google owns YouTube, the Android operating system, and Google Ads, among other products. The company operates under its parent, Alphabet Inc., which was formed in 2015 to manage its diverse portfolio and innovation-driven projects such as Waymo, Verily, and DeepMind. Google is also known for its ambitious initiatives in artificial intelligence, virtual reality, and sustainable technology solutions.

Google Cloud Platform (GCP) is a public hybrid cloud that is hosted on Google Common Infrastructure (GCI), serving the US Federal Government, personal users, and other organizations. GCI is responsible for implementation of common controls for all Google service offerings, including GCP.

Google Workspace, previously known as G Suite, is a suite of cloud-based productivity and collaboration tools designed to improve organizational efficiency, enhance team collaboration, and streamline communication. It combines core applications like Gmail, Google Drive, Google Calendar, Google Meet, and Google Docs, alongside a suite of collaborative tools, into a cohesive platform optimized for flexibility, scalability, and security.

Its ease of use, coupled with strong cloud integration and accessibility, makes it especially attractive to startups, small businesses, and remote workforces. By choosing Google Workspace, organizations benefit from a trusted platform that can adapt to evolving business needs, streamline collaboration, and support digital transformation efforts.

Google Workspace is built and managed on GCI, which is the combination of people, processes, technologies and facilities that Google relies on. GCI consists of multiple reusable technologies such as databases, compute power, management tools, and security controls, abstracting these components to a common layer means that Google evidenced they can apply strong data protection and security controls across the entire environment and service offerings.

Inclusive within scope of the Google Cloud Platform assessment is Google Cloud VMware Engine (GCVE) which is a managed VMware as a service product offering purpose built for ground up and migrated VMware workloads on Google Cloud, GCVE enables enterprise customers to run VMware virtual machines natively in a dedicated, private Software Defined Datacentre (SDDC) within Google Cloud.

GCVE shares Google common governance controls throughout the organization and platform however there are nuances at the hardware and facilities layer that will be identified within sub sections of this report.

[1] https://www.google.com/intl/en_au/search/howsearchworks/our-approach/

bernard@protonmail.ch

Google engaged Sekuro to perform an IRAP Assessment of Google Cloud Platform and Google Workspace between August 2024 and December 2024.

bernard@botmaker.io

1.2 Implementation Summary

The Australian Government Information Security Manual (ISM) defines the framework and controls that organisations providing services to government agencies should align with to ensure cyber security. The aim is to protect systems and information from cyber threats using risk management principles.

During the assessment the following were identified:

Google Cloud Platform: 48 alternative controls, 0 not implemented controls, 28 ineffective controls and 2 no visibility controls.

Google Cloud VMware Engine: 49 alternative controls, 0 not implemented controls, 28 ineffective controls and 2 no visibility controls.

Google Workspace: 48 alternative controls, 0 not implemented controls, 26 ineffective controls and 2 no visibility controls.

These findings are presented in Section 1.3 Authorisation Considerations of the report. Google has implemented satisfactory security controls that encompass the fundamentals of policies, processes, and technologies as per the ISM's guidelines. The controls are considered adequate to ensure cyber security for Australian Government entities.

As part of its commitment to provide service to Australian Government entities, Google acknowledges the need for independent and comprehensive Cloud Security Assessment. The assessment aligns with the Australian Government's ISM.

The evaluation has identified vulnerabilities that need to be taken into consideration by government entities to assess the suitability of Google Cloud Platform and Google Workspace. Section 6, Key Assessment Findings, details the vulnerabilities identified. Government entities are encouraged to consider these findings when making decisions about using Google Cloud Platform and Google Workspace.

Google was assessed against the March 2024 version of the ISM, as such, Figure 1 illustrates the compliance[2] extracted from the Cloud Controls Matrix (CCM).

bernardobermudez.io

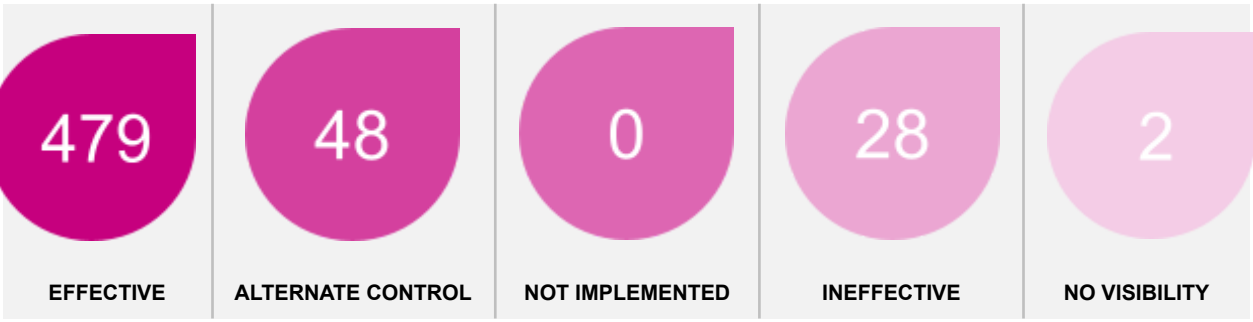


Figure 1: Google Cloud Platform Compliance Summary

[2]Alternate Control – The CSP is effectively meeting the control's objective through an alternate control.
Effective – The CSP is effectively meeting the control's objective.
Ineffective – The CSP was not found to be adequately meeting the control objective.
Not Implemented – The CSP has decided not to implement the control.
No Visibility – The assessor was unable to obtain adequate visibility to assess the control implementation.

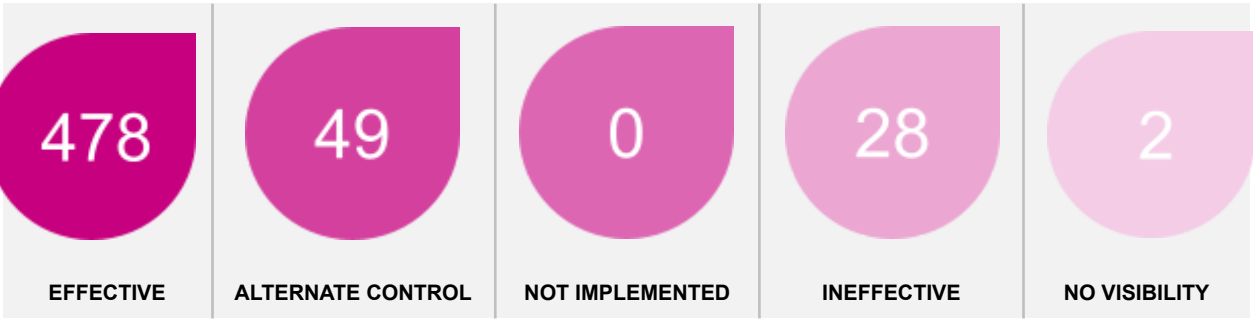


Figure 2: Google Cloud VMware Engine Compliance Summary

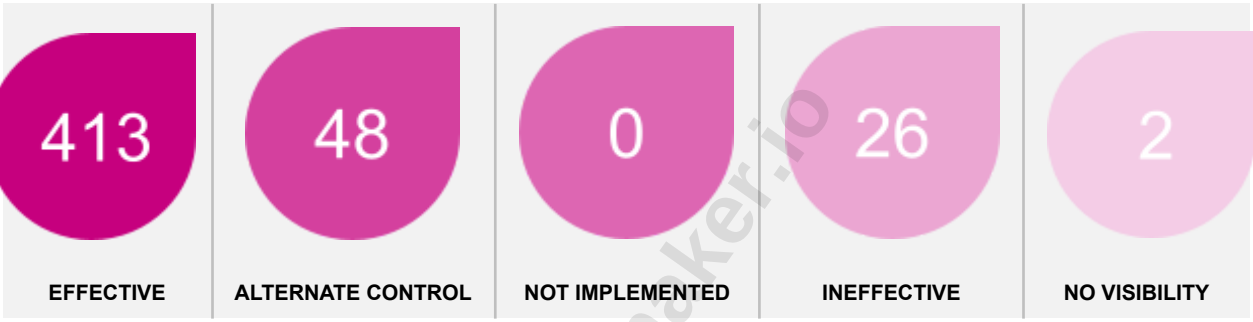


Figure 3: Google Workspace Compliance Summary

The Assessor confirms that based on findings, observations, and interviews conducted, Google Cloud Platform, Google Cloud VMware Engine and Google Workspace is designed, implemented, and operated in accordance with the Australian Cyber Security Centre (ACSC) ISM requirements. The overall architecture, technology in use, policy, standards, and operating procedures remains operational and functional.

bernard@dpmaker.io

1.3 Authorisation Considerations

The Assessor, through various testing procedures and workshops has gained confidence that Google Cloud Platform and Google Workspace are designed and operating effectively to achieve the requirements stipulated in the March 2024 version of the ISM.

Google have demonstrated maturity of their information security capabilities and have proven through various compliance regimes, their ability to conduct business in a secure manner.

For the context of this report it is noted that Google is both the outsourced cloud service provider and the cloud service provider.

The assessment has identified the following ineffective controls applicable to GCP, GCVE and Workspace:

- ISM-1737, ISM-1638 - The information captured within these registers are not in alignment with the ISM requirements for service registers. Information such as contact details, classification of data handled, due dates for next security assessments are captured across Buying Hub portals/categories and within contractual agreements.
- ISM-1571 - The evidence reviewed supplied by Google did not meet the requirements set out in this ISM control to ensure the right to verify compliance with security requirements is documented in contractual agreements, it is noted by the assessor whilst it is not documented evidence was provided that the process is developed and carried out on a regular basis.
- ISM-1163 - Continuous monitoring plans are defined and captured within the SSP appendices (GCP, GCI, Workspace) and were made available to the Assessor for review. However it was noted some misalignment with the ISM controls such as vulnerability scans are carried out monthly rather than the control requirement of fortnightly and penetration testing is carried out annually rather than prior to deployment of the product or carrying out significant changes.
- ISM-1724, ISM-0361 - The assessor reviewed Google's destruction process at time of physical walkthrough's and noted that the equipment used to destroy magnetic hard disks was not one listed within this control, A SEM manufactured punch machine is used to damage the disk and platters. However these controls are not applicable to Google Workspace.
- ISM-1874 - Whilst Multifactor authentication is the responsibility of the consumer Google Workspace offers a wide range of options for consumers to utilize to ensure a phishing resistant approach is adopted, This includes hardware-based solutions such as FIDO2 keys and mobile device authentication. However non-phishing resistant options are also available for use such as TOTP.
- ISM-1698, ISM-1699, ISM-1700, ISM-1701, ISM-1702, ISM-1752, ISM-1703, ISM-1900 - The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool. The 3PAO also

jeremiah@tesumaro.jp

regularly audits Google's internal scan tools to ensure that they are working correctly.

- ISM-0859, ISM-0991 - The assessor identified that application logs, including those records that detail security-relevant events, are retained for at least one year.
- ISM-1183 - The assessor reviewed the SPF record used for email, Google's SPF is currently set to ~all which indicates a soft fail is used which does not meet the requirement laid out for hard fail.
- ISM-1311 - Within the Google Production environment it was noted from Technical walkthroughs that the use of SNMP version 2 is used.
- ISM-0471 - The list of cryptographic algorithms reviewed showed that 3DES is still enabled within the environment which is not a supported algorithm.
- ISM-1139 - Customer core content data is encrypted between customer clients and Google, between Google data centers and at rest. Encryption between an agency customer and Google servers is dependent on the customer's client configuration, However it was identified that older versions of TLS are still in use which does not meet the requirement of using the latest.
- ISM-1369 - Whilst AES-GCM is in order the preferred encryption method it is noted that AES-CBC is still enabled. It was also reviewed that TLS_RSA_WITH_3DES_EDE_CBC_SHA is still enabled.
- ISM-1373 - It was identified that TLS_RSA_WITH_3DES_EDE_CBC_SHA is used within the environment, This key exchange algorithm does not support Perfect Forward Secrecy (PFS) which is recommended, so attackers cannot decrypt the complete communication stream leading to MITM attacks.
- ISM-1375 - The assessor reviewed the configuration of the Google servers and noted that whilst SHA-2 is used and preferred SHA is still enabled.
- ISM-1453 - The IRAP assessor identified the presence of Perfect Forward Secrecy enabled cipher suites in the evidence reviewed. However TLS_RSA_WITH_3DES_EDE_CBC_SHA is still enabled This key exchange algorithm does not support Perfect Forward Secrecy (PFS).
- ISM-1293 - Google does not perform content filtering or application of security controls based on the content of the data packet. However as part of the traffic monitoring random data packets are monitored to verify if the actual payload is encrypted or not. Decrypting network traffic to perform content analysis would be contradictory to the Google security policy of encrypting all network traffic.

The assessment has identified the following No Visibility controls applicable to GCP, GCVE and Workspace:

- ISM-0140 - The Google team identified during the assessment that this process is currently under development and was not able to provide evidence.
- ISM-1783 - At the time of the assessment the assessor was unable to identify if Public IP addresses controlled by, or used by, an organisation are signed by valid ROA records.

bernard@scimaker.io

The assessment also identified areas where Google has implemented alternative controls to meet the intent of the in-scope ISM controls; these can be found in Table 7.

The assessor confirms that the environment is built on sound security principles. Customers consuming Google Cloud Platform Google Workspace and Google Cloud VMware Engine services should review documentation provided by Google prior to consuming the service.

Chris Ekert

Chris.Ekert@sekuro.io

00326

Sita Bhat

Sita.Bhat@sekuro.io

00333

Prashant Haldankar

Prashant.Haldankar@sekuro.io

00054

bernard@botmaker.io

2 Introduction

2.1 Cloud Service Provider[3]

Google, as a Cloud Service Provider (CSP), offers a comprehensive suite of cloud computing services through the Google Cloud Platform (GCP). GCP encompasses Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings, all built on the robust foundation of Google's Common Infrastructure (GCI). This infrastructure provides a secure and scalable environment for Google's diverse product portfolio, including Google Workspace, YouTube, and Android. Google's commitment to security and innovation is evident in its continuous development of advanced technologies and tools designed to enhance user safety, data protection, and threat detection. Through GCP, Google empowers businesses and individuals to leverage the power of the cloud for enhanced productivity, collaboration, and data management. Google Cloud Platform (GCP) comprises IaaS, PaaS and SaaS offerings that sit on top of Google Common Infrastructure.

2.2 Cloud Service Platform[4]

2.2.1 Overview

Google maintains a private cloud Infrastructure as a Service referred to as Google Common Infrastructure (GCI) upon which its product offerings are built. In addition to providing a technical infrastructure for products to run, GCI provides common processes such as security training, change management, secure software development (SDLC), vulnerability management and risk management. The Google Common Infrastructure consists of four components that make up the Google application stack, these are listed below:

- Network,
- Data Centres
- Resource management, and
- Data Storage

Google Workspace is built and managed on Google Common Infrastructure (GCI), which is the combination of people, processes, technologies and facilities that Google rely on. GCI consists of multiple reusable technologies such as databases, compute power, management tools, and security controls, abstracting these components to a common layer means that Google evidenced they can apply strong data protection and security controls across the entire environment and service offerings.

Google Cloud Platform (GCP), a public hybrid cloud, is hosted on Google Common Infrastructure (GCI). GCI implements common controls for all Google service offerings, including GCP, which serves the US Federal Government, personal users, and other organizations.

GCVE is a managed service from Google Cloud that allows businesses to run VMware-based workloads natively on Google Cloud infrastructure. GCVE is designed to enable companies to migrate or extend their on-premises VMware environments to the cloud

[3] For the purpose of this IRAP assessment, the Cloud Service Provider (CSP) is the IT company that provides the on-demand, scalable computing resource, product etc. in this instance, the CSP is Google.
[4] For the purpose of this IRAP assessment, the Outsourced Cloud Service Platform (OCSP) is the third-party company that provides the hosting infrastructure i.e., physical data centre, environmental safeguards etc. in this instance the OCSP is Google.

without needing to refactor or modify their applications, leveraging the familiarity and functionality of VMware tools while gaining the scalability and flexibility of Google Cloud.

Google Workspace runs on the same binaries and security controls across all editions.

The Google Workspace editions, cloud offering model and targeted users are listed below.

- Google Workspace Business Starter: Productivity suites for businesses with 1-300 users. Professional productivity suite with 30 GB pooled storage per user*
- Google Workspace Business Standard and Plus: Productivity suites for businesses with 1-300 users, Standard offers Enhanced productivity suite with 2 TB pooled storage per user, while plus offers Advanced productivity suite with 5 TB pooled storage per user.
- Google Workspace Enterprise Plus: Marketed to Government and enterprise whilst adding premium security and advanced controls for unlimited users.
- Google Workspace Enterprise Standard: Marketed to Government and enterprise and it comprised all Google Workspace Services except Google Cloud Search and Workspace Add-ons.
- Google Workspace for Education: Marketed to education institutions and is a discounted suites for qualifying educational institutions.
- Google Workspace Frontline: Marketed to frontline workers, this edition comprises all the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, Google Workspace Migrate and the Workspace Add-ons.

bernard@kotmaker.ro

2.2.2 Logical Diagram

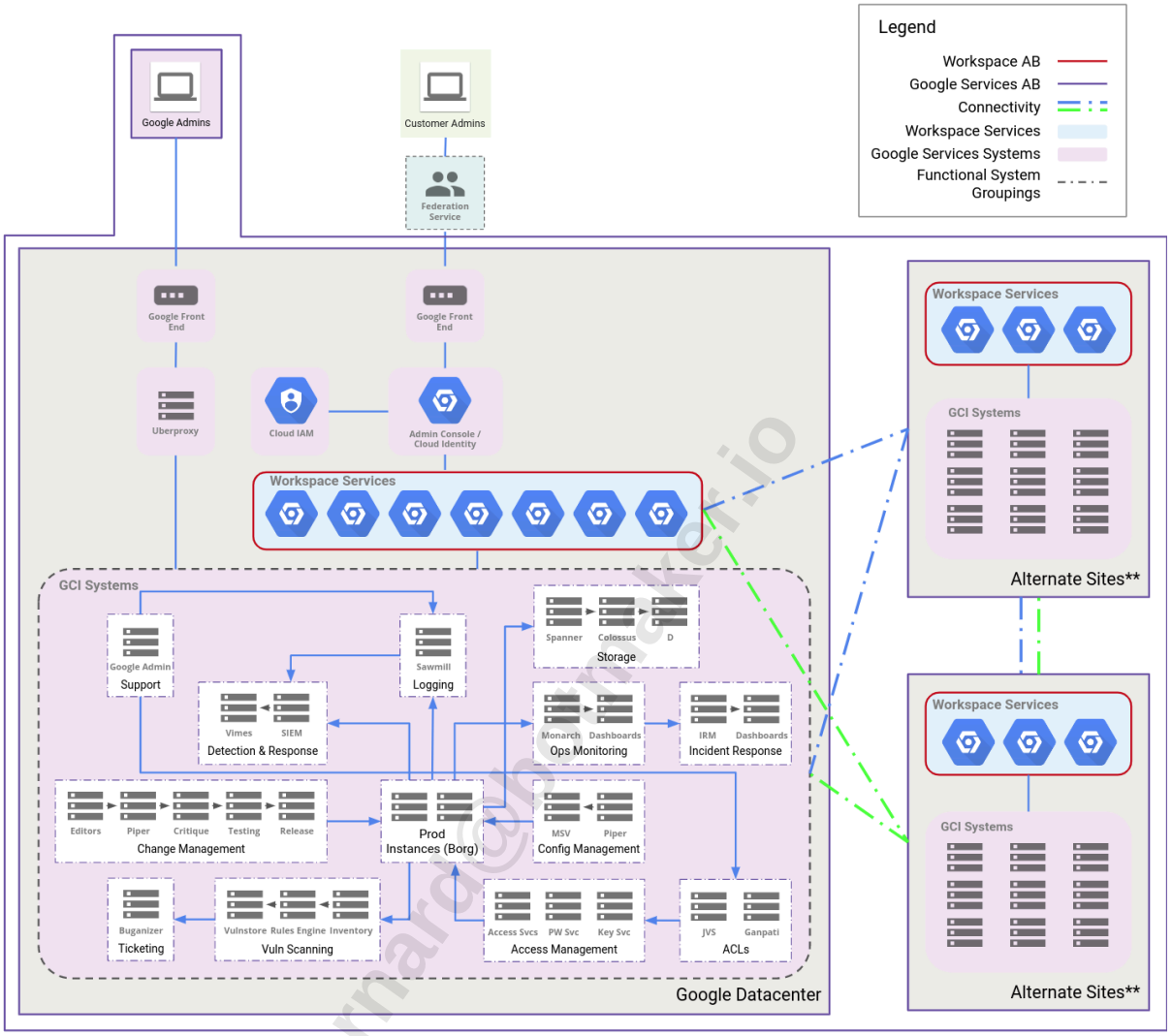


Figure 4: Workspace - Logical Diagram showing authorisation boundary for assessment

bernard@sekuro.io

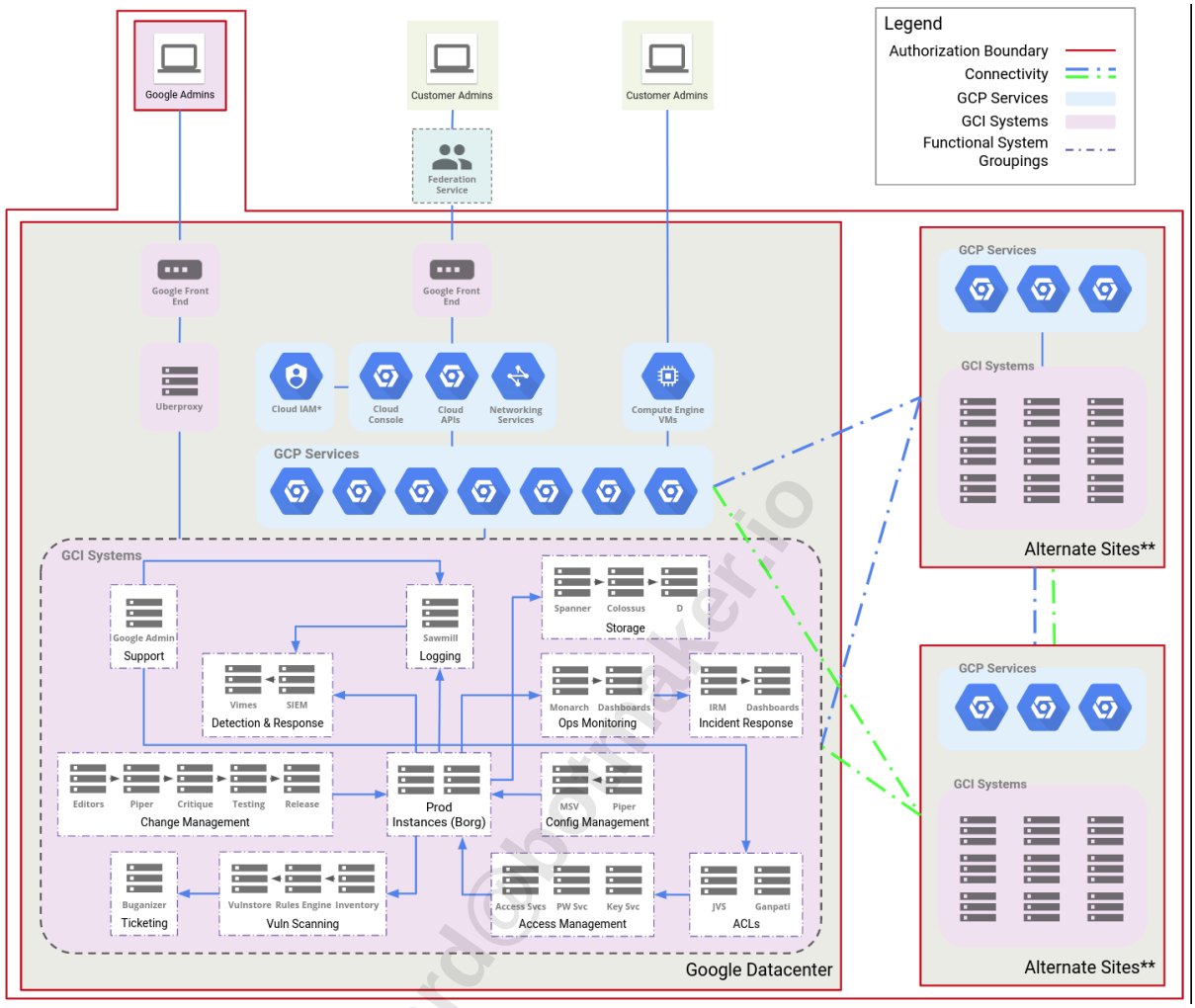


Figure 5: Google Services - Logical Diagram showing authorisation boundary for assessment

bernardo@silverio

3 Assessment Details

3.1 Methodology

This report does not constitute as legal advice and should not be relied upon as such.

The methodology for the assessment performed for Google are based on the ACSC cloud security guidance and ISM requirements and guidance.

The following IRAP assessment steps were taken:

- Confirming the intended security classification of the data to be managed by Google, i.e., PROTECTED.
- Identifying the authorisation boundary or network segmentation between Google environments. Refer to Section 2 Introduction.
- Gaining an understanding of Google Workspace and GCVE and its purpose.
- Identifying the sources of information, locations, and evidence required to complete the assessment i.e., on-site components
- Identifying assessment methods (such as interviews, video conferencing, etc.) and determining the procedure for verifying information and evidence.
- Obtaining evidence of the implementation of the March 2024 ISM PROTECTED controls and their effectiveness.
- Identifying if Google has implemented an alternative security control and determining the intent of this security control and how it meets the purpose of the security control in the ISM.
- Documenting any 'Not Implemented' or 'Ineffective' ISM security controls and how the absence of these security controls is currently mitigated by Google.
- Provide recommendations to mitigate the risk of absence of ISM security controls that have not been risk mitigated by Google.
- Documenting the assessment using the Cloud Security Assessment Report Template and the CCM provided by the ACSC.
- Identifying and perceived or potential conflicts of Interest and lodging with ASD.

kamal@botmaker.io

3.2 Scope

3.2.1 Dependencies and Inheritance

Due to the size and complexity of Google and its various environments, dependencies may vary over time. For a managed list of Components and Dependencies refer to section 5.1.4.

3.2.2 CSP Locations

Google's main headquarters, often referred to as the Googleplex, is located in Mountain View, California. However, the company has numerous offices worldwide, spanning across North America, South America, Europe, Asia, the Middle East, and Australia. These offices serve as hubs for various functions, including engineering, sales, marketing, and operations, contributing to Google's global reach and impact. For a full list of office locations refer to the publicly maintained list of Google Offices[5].

3.2.3 Service Regions

Google Cloud products are served from specific regional failure domains and are fully supported by Service Level Agreements to ensure you are designing your application architecture within the structure of Google Cloud.

Google Cloud infrastructure services are available in locations across North America, South America, Europe, Asia, the Middle East, and Australia. These locations are divided into regions and zones. You can choose where to locate your applications to meet your latency, availability, and durability requirements.

Google Workspace is hosted on Google's global infrastructure, which includes data centers geographically located around the world, therefore Australian Government Agencies should take into consideration the risks and implications of storing data in US datacenters. As an administrator, you can use data regions to store your covered Google Workspace data in a specific geographic location. Your location options are the United States, Europe, or No preference.

Global Internal Services can run in or be replicated in the following cloud regions:

Americas

- southamerica-west1
- us-central1
- us-east1
- us-east4
- us-west1
- us-west4

Europe

- europe-north1
- europe-west1
- europe-west4

[5] https://about.google/locations/?region=asia-pacific

bernard@normaker.io

Asia

- asia-east1
- asia-southeast1

3.2.4 Cloud Services

As part of the IRAP assessment carried out the following services were included:

Google Cloud Platform Services in scope of this assessment
Admin Console
Alert Center API
Apps Script
Assignments
Calendar Resource API
Classroom
Cloud Identity
Cloud Search
Data Transfer API
Directory API
Domain Shared Contacts API
Drawings
Email Audit API
Enterprise License Manager API
Gemini for Workspace
Gemini {Google Workspace Enterprise}
Gmail
Gmail Rest API
Google Calendar
Google Calendar API
Google Chat
Google Contacts
Google Docs
Google Drive
Google Drive Activity API
Google Drive Rest API
Google Forms
Google Groups

bernard@botmaker.io

Google Jamboard
Google Keep
Google Meet
Google Sheets
Google Sheets API
Google Sites
Google Slides
Google Tasks
Google Tasks API
Google Vault
Google Vids
Google Voice
Google Workspace Migrate
Groups Migration API
Groups Settings API
Mobile Device Management
People API
Read Along
Reports API
Reseller API
SAML-based SSO API
Secure LDAP
Security Center

bernard@botmaker.io

Table 1: Google Workspace Services

Google Cloud Platform Services in scope of this assessment
Access Approval
Access Context Manager
Access Transparency
Advanced API Security
Agent Assist
AI Platform Deep Learning Container
AI Platform Training and Prediction
AlloyDB

Anti-Money Laundering AI
API Gateway
Apigee
App Engine
Application Integration
Artifact Analysis
Artifact Registry
Assured Workloads
AutoML Natural Language
AutoML Tables
AutoML Translation
AutoML Video
AutoML Vision
Backup and DR Service
Backup for GKE
Bare Metal HSM
Bare Metal Rack HSM
Batch
Chrome Enterprise Premium
BigQuery
BigQuery Data Transfer Service
BigQuery Omni
Binary Authorization
CCAI Platform
Certificate Authority Service
Certificate Manager
Google Security Operations (SIEM)
Google Security Operations (SOAR)
Cloud Armor {NetLB}
Cloud Asset Inventory
Cloud Bigtable
Cloud Billing
Cloud Build
Cloud CDN
Cloud Composer

bernard@botmaker.io

Cloud Console
Cloud Console App
Cloud Data Fusion
Cloud Deployment Manager
Cloud DNS
Cloud Endpoints
Cloud External Key Manager (Cloud EKM)
Cloud Filestore
Cloud NGFW (formerly Cloud Firewall)
Cloud Functions
Cloud Functions for Firebase
Cloud Healthcare
Cloud HSM
Cloud IDS (Cloud Intrusion Detection System)
Cloud Interconnect
Cloud Key Management Service
Cloud Life Sciences
Cloud Load Balancing
Cloud Load Balancing {L4 ILB}
Cloud Load Balancing {L7 ILB}
Cloud Load Balancing {Network Load Balancing}
Cloud Logging
Cloud Monitoring
Cloud NAT (Network Address Translation)
Cloud Natural Language API
Cloud Org Policy
Cloud Profiler
Cloud Router
Cloud Run
Cloud Scheduler
Cloud Service Mesh
Cloud Shell
Cloud Source Repositories
Cloud Spanner
Cloud Speaker ID

bernard@botmaker.io

Cloud SQL
Cloud Storage for Firebase
Cloud Tasks
Cloud Trace
Cloud Translation
Cloud Vision
Cloud VPN
Cloud Workstations
Compute Engine
Compute Engine {VM Manager}
Connect
Contact Center AI (CCAI)
Contact Center AI Insights
Container Registry
Data Catalog
Database Migration Service
Dataflow
Dataform
Dataplex
Dataproc
Dataproc Metastore
Datastore
Datastream
Dialogflow
Discovery Solutions
Document AI
Document AI Warehouse
Error Reporting
Eventarc
Firebase App Check
Firebase Authentication
Firebase Test Lab
Firestore
Food Ordering AI Agent
Gemini for Google Cloud

bernard@botmaker.io

Generative AI on Vertex AI
GKE Enterprise Config Management
GKE Identity Service
Google Cloud Armor
Google Cloud Deploy
Google Cloud Identity-Aware Proxy
Google Cloud Marketplace
Google Cloud SDK
Google Cloud Storage
GTI for Google Security Operations
Google Cloud VMware Engine (GCVE)
Google Earth Engine
Google Kubernetes Engine
Google Threat Intelligence
Healthcare Data Engine
Hub
Identity & Access Management (IAM)
Identity & Access Management (IAM){Workforce Identity Federation BYOID}
Identity Platform
Infrastructure Manager
Integration Connectors
Key Access Justifications (KAJ)
Knative serving
Looker (Google Cloud core)
Looker Studio
Managed Service for Microsoft Active Directory (AD)
Media CDN
Memorystore
Memorystore {Memorystore for Memcached}
Memorystore {Memorystore for Redis}
Migrate to Virtual Machines
Migration Center
Network Connectivity Center
Network Intelligence Center
Network Service Tiers

bernard@botmaker.io

Persistent Disk
Personalized Service Health
Privileged Access Manager
Policy Controller
Pub/Sub
Qwiklabs
Ray on Vertex
reCAPTCHA Enterprise
Recommendations AI
Recommender
Resource Manager API
Retail Search
Risk Manager
SecLM
Secret Manager
Secure Source Manager
Security Command Center
Sensitive Data Protection (including Cloud Data Loss Prevention)
Service Directory
Service Infrastructure
Service Mesh
Speech-to-Text
Storage Transfer Service
Tables
Talent Solution
Text-to-Speech
Traffic Director
Transcoder API
Vertex AI Codey
Vertex AI Colab Enterprise
Vertex AI Conversation
Vertex AI Data Labeling
Vertex AI Platform
Vertex AI Search
Vertex AI Workbench Instances

bernard@botmaker.io

Video Intelligence API
Virtual Private Cloud
VirusTotal
VPC Service Controls
Web Risk API
Workflows
Workload Manager
Vertex AI {Online and Batch Prediction}
Vertex AI {Vertex AI Forecast}
Vertex AI {Vertex AI Model Registry}
Vertex AI {Vertex AI Workbench User Managed Notebooks}
Vertex AI {Vertex ML Metadata}
Vertex AI {Vertex Model Monitoring}
Vertex AI {Vertex Pipelines}
Vertex AI {Vector Search}
Vertex AI {Vertex Training}

Table 2: Google Cloud Platform Services

richard@botmaker.io

3.2.5 Exclusions

ISM controls that apply at SECRET and TOP SECRET classification levels and ISM controls that are deemed out of scope for this IRAP assessment, have been marked as *Not Applicable* within the CCM, which can be found in Appendix A. However, it should be noted that certain ISM categories are deemed *Not Applicable* (as demonstrated below), although the ISM Guideline in its entirety may not be out of scope.

ISM guideline	ISM sub-category	Justification
Guidelines for Communications Systems	Telephone Systems Video conferencing and Internet Protocol telephony Fax machines and multifunction devices	This is not applicable as telephone systems, video conferencing, internet protocol telephones, fax machines, and multi-functional devices were out of scope as the Google Cloud Platform and Google Workspace environment does not leverage or provide these functionalities.
Guidelines for Evaluated Products	Evaluated product procurement Evaluated product usage	This is not applicable to Google as SECRET and TOP SECRET information is not used or processed within the Google Cloud Platform and Google Workspace environment and further was not procured during the assessment as the Google Cloud Platform and Google Workspace assessment was carried out at the PROTECTED level.
Guidelines for Cryptography	Internet Protocol Security	This is not applicable as Google does not have a requirement to use high assurance cryptographic algorithms. Further, there is no VPN involved in

ISM guideline	ISM sub-category	Justification
	Secure/Multipurpose Internet Mail Extension	administering the commercial service because Google uses its variant Zero Trust.
Guidelines for Enterprise Mobility	Mobile Device Management Mobile device usage	This is not applicable as any mobile devices used by Google personnel are not in scope of Google Cloud Platform and Google Workspace services, due to the network segregation applied between the corporate environment of Google i.e., network rules enforced by Google's gateways and Google's various production environments.
Guidelines for Gateways	Diodes Peripheral switches	This is not applicable as diodes and peripheral switches are not used by Google as part of the Google Cloud Platform and Google Workspace environment.
Guidelines for Networking	Wireless networks	This is not applicable as wireless devices are not in scope for the assessment of Google Cloud Platform and Google Workspace environment.

Table 3: Exclusions

bernard@botmaker.ro

4 CSP Security Fundamentals Assessment

4.1 Security Culture

Throughout the assessment, Google demonstrated that a risk-based approach is taken throughout the organisation, with information security at the forefront of conducting business. Section 4.2.2 Enterprise Risk Management further details how Google provides support for measuring and achieving its security obligations, which aligns the business to deliver its strategic goals.

Google's culture, values, responsibilities and expected behaviour regarding system usage are all covered within the Code of Conduct. If an employee performs a breach of the Code of Conduct with Google, a formal disciplinary process may take place through the Legal and HR departments. If this breach requires terminating or change of employment responsibilities, the information security responsibilities, including confidentiality, remain in the employment contractual arrangements. Actions for disciplinary or insider threats are coordinated between Legal and HR. The appropriate action is determined depending on the nature of the threat. Accounts are removed or suspended before leaving the company. Before conducting any work with Google, employees are required to sign a confidentiality agreement agreeing to not disclose any proprietary information. Additionally, new employees to Google are required to undertake a third-party background check commensurate to their role or job responsibilities.

Google products have mature System Development Life Cycle (SDLC) processes with a thorough set of security activities spanning their software development practices, processes and tools. Google's SDLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, deployment, and incident response. This ensures Google can respond to weaknesses reported in their products to issue emergency updates and assistance as required. For more details on the System Development Life Cycle, refer to Section 4.2.11.

Google ensures all employees are provided with adequate and targeted information security awareness training, detailed in Section 4.2.3 Personnel Security of this report; this is achieved by a mandated annual Google wide security awareness training program as part of the ISMS implementation. As detailed in 4.1.6 Information Security Compliance Certifications, Google is dedicated to conducting continuous improvement throughout all its relevant compliance regimes.

4.1.1 Strengths

Throughout this assessment, Google has been evidenced as an organisation that places a strong emphasis on security and has implemented a positive security culture across its operations. As part of this culture, the company has designed and implemented various controls to monitor the ongoing effectiveness of its security measures. These controls are continuously monitored to identify and address potential failures that could lead to controls not operating as expected.

Google's security culture includes a focus on ongoing training and education to ensure that employees are aware of potential security risks and best practices for mitigating them.

renew@normkey.ro

Additionally, the company engages in regular security assessments and testing to identify potential vulnerabilities and ensure that its security controls are effective.

Overall, Google's security measures are designed to protect its customers' sensitive data and maintain the integrity of its systems. By incorporating a comprehensive security culture and continuously monitoring its controls, Google can stay ahead of emerging threats and respond quickly to any potential security incidents. For more information on Google's security practices and measures, please refer to the sections of the report listed below.

- Section 4.1: Security Culture
- Section 4.2: Governance
- Section 4.3: Administrative and Support Environment
- Section 4.4: CSP's Cloud Protection Environment

4.1.2 Weaknesses

At the time of the assessment Google Cloud Platform and Google Workspace did not present any significant technical or operational weaknesses. However, Section 6 Key Assessment Findings outlines the implementation for Google Cloud Platform and Google Workspace and any significant control anomalies.

4.1.3 Response to Cyber Security Incidents

At the time of the assessment there were no notable cyber security incidents within the Google Cloud Platform and Google Workspace. In addition to this, Google's incident response is outlined in Section 4.2.10 of this report.

4.1.4 Contributions to Cyber Security

Google significantly contributes to cybersecurity through its research, products, and tools designed to enhance user safety, data protection, and threat detection. Here are some key areas of Google's impact on cybersecurity:

- **Google Safe Browsing:** This service protects users across the web by warning them of potentially dangerous sites, phishing attempts, and malware. It works on Chrome, Firefox, and other major browsers.
- **Google Titan Security Keys:** These hardware tokens are designed to protect accounts with physical verification, improving protection against phishing.
- **Google Cloud Security Products:** Google Cloud provides security solutions such as Identity and Access Management (IAM), data encryption, DDoS protection, and security monitoring for businesses using Google Cloud.
- **Project Zero:** Google's elite security team, Project Zero[6], focuses on identifying and reporting "zero-day" vulnerabilities (unknown security flaws) to improve the security of widely used software across industries.
- **Open-Source Security Tools:** Google develops and maintains open-source tools like Tsunami[7] (vulnerability scanner) and GRR (incident response

[6] https://googleprojectzero.blogspot.com/

[7] https://opensource.googleblog.com/2020/06/tsunami-extensible-network-scanning.html

bernard@bottmaker.io

framework), which help researchers and companies enhance their cybersecurity defences.

Overall, Google is a major player in cybersecurity through its wide-ranging products, research initiatives, partnerships, and public education efforts. Its investments in cloud security, AI-driven threat detection, and user protection help enhance cybersecurity resilience worldwide. Furthermore, Google actively contributes to the broader cybersecurity landscape through initiatives like Google Safe Browsing, Titan Security Keys, Project Zero, and open-source security tools. These efforts underline Google's dedication to fostering a safer and more secure online environment for all.

4.1.5 Cyber Security Guidance

Google provides extensive cybersecurity guidance aimed at protecting individuals, businesses, and developers from online threats. Google's Safety Centre[8] is a dedicated online resource providing information, tools, and guidance to help users stay safe online. It covers essential topics like privacy, security, and digital well-being, making it accessible for users of all levels to understand and protect themselves in the digital world.

Furthermore, Google provides product specific security checklists and best practices based on various factors such as business size, industry type and locations.

4.1.6 Information Security Compliance Certifications

Google's commitment to compliance is evident in the various certifications it holds for Google Workspace, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27701, and IRAP Assessed at Protected. To support this IRAP assessment, Google holds the following certifications for Google Workspace:

- ISO/IEC 27018:2019
- ISO/IEC 27001:2013
- ISO/IEC 27017:2015
- ISO/IEC 27701:2019
- ISO/IEC 27001:2022
- IRAP Protected
- CSA STAR
- C5:2020
- SSAE18 - SOC 1 (Service Organization Controls Report)
- SSAE18 - SOC 2 AICPA Trust Service Criteria
- SSAE18 - SOC 3 AICPA Trust Service Criteria
- ENS (National Security Framework) Spain
- Multi-tiered Cloud Computing Security Management System (MTCS)
- OSPAR
- GNS – Portugal

[8] https://safety.google/

bernard@otmaker.io

bernard@botmaker.io

4.2 Governance

4.2.1 Enterprise Risk Management

Google conducts risk assessments to identify threats to systems as well as vulnerabilities that could potentially affect the confidentiality, integrity and availability of systems. Many of these risk management activities are embedded into the team's day-to-day operations, whilst other risk identification and assessment activities occur during security design reviews, the OKR evaluation process, compliance evaluations or ad-hoc reactions to emerging industry issues.

The process for conducting risk assessments and determinations is consistent with guidance provided in NIST SP 800-30 Rev1 documentation. Google expresses risks identified universally across the organisation as either High, Medium or Low priority. Risks may be assessed qualitatively and / or quantitatively as appropriate.

Google teams acknowledge the need to follow due process, and teams also place additional consideration on the following:

- The likelihood of a given threat-source attempting to exercise a given vulnerability
- The magnitude of the impact should be a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing controls for reducing or eliminating risk
- The likelihood that a potential vulnerability could be exercised by a given threat-source described as High, Medium or Low.

The Google Security team assists the engineering teams with managing security risks, Security Team members may also be embedded with engineering teams to assist on projects ensuring risks are identified at all stages of the project life cycle. Furthermore, the Security team's interaction with engineering teams provides a central point for security risk aggregation and analysis.

Google aims to effectively manage risks and protect Google's production environment by performing security and privacy design reviews, security assessments, code reviews, security monitoring, incident response, detection tools and embedding security in engineers within the operational teams. The Security Operations (SecOps) group within the Security team identifies and responds to risks identified in day-day operations and through ongoing monitoring processes. SecOps collaborates with several other security teams at Google in order to leverage existing expertise and tooling.

4.2.2 Personnel Security

Google has developed, implemented and maintained an Information security program that is a requirement of all personnel to complete as part of onboarding and annually thereafter. Google's Risk, Compliance and Integrity team monitors compliance with Google Privacy and Information Security training, Records of training completion are maintained.

The Privacy and security training is designed to raise awareness of Google's information assets and how Google expects personnel to protect these assets. In addition to the Privacy and Information Security training Google promotes awareness through a variety of additional means:

bernat@pctmaker.io

- **Noogler Training:** Google provides training to all new hires (Nooglers) during onboarding and orientation in order to review the requirements of the Google Security Policies.
- **Security Site:** Google maintains an easily accessible internal website that is the central point for many security related resources including links to policies and guidelines.
- **Interactive Training:** Google has developed an interactive internal code lab that teaches engineers about common web security vulnerabilities. This code lab has also been made available to the public.
- **Advanced Security Education:** Google has developed a training program called Resident Hacker, that teaches advanced topics in computer security including web security, common programming language security and practical cryptography.
- **Security Newsletter:** A periodic newsletter (OWND) is distributed with alerts and tips on security matters related to Google products, Coding practices and general awareness matters.

Google's onboarding process is highly automated, with all new hires required to complete and pass a pre-employment background check which is outsourced to an external vendor HireRight. Disciplinary actions related to policy violations are investigated by cross functional teams and depending on the severity, sanctions could range from written warnings to termination. Google employees can apply for internal roles advertised within Google's Grow platform, on success an employee's role is internally transferred, and their systems access is updated to reflect their new role and responsibilities.

4.2.3 IT Change Management

Google analyses changes to network devices within the environment to determine potential security or availability impacts prior to change implementation. Changes are subject to review and approval, unit tests and pre-change automatic validation. Additionally, Access Control List (ACL) changes are reviewed and approved by the Google Security Team prior to being pushed into production. Network configuration changes are implemented through a gradual rollout process spread over several days. This allows for any issues to be detected early and managed, following this phase a controlled, rate-limited deployment continues across the network. Any systematic failures are managed by the network security team.

Google maintains visibility of changes to machines to identify potential security or availability impacts that may arise prior to the implementation. Changes that may have significant risk to production get reviewed and approved during a weekly Internal office meeting. Additionally, changes are released in small batches to a set of qualification machines and then to a larger set ensuring that any impacts are detected early and remediated or rolled back. Post these phases changes are continued to be rolled out to the rest of the production environment over a two-week period.

4.2.4 Data Type Definitions

Google has three data classifications which are detailed in Table 3 below; Need-to-Know (NTK), Confidential, and Public. Suitable guidance is provided to all staff through policy and

bernardo@ctmaker.io

ongoing security awareness training to ensure data is appropriately classified, protected, access, and shared.

Classification	Description
Need-to-Know data	Need-to-Know data is sensitive legal, business, and financial information that only certain individuals need to know to do their jobs. People in different roles and working on different projects or Product Areas, or Bets need access to different information. Share Need-to-Know information only with people who need it to fulfill their specific job responsibilities.
Confidential data	Confidential data is non-public technical, business, and product information that is appropriate to disclose broadly within Google or a Bet, in line with business purposes.
Public data	Public data is information that, with appropriate authorization, has explicitly and intentionally been made available to the public. If you work with Public data, you are responsible for ensuring its integrity and accuracy, and handling it consistent with any legal restrictions.

Table 4: Google Data Classifications

4.2.5 Data Protections

Google uses a proprietary distributed file system across the entire GCI environment, based on the architecture where redundancy spreads the load of services and data across multiple underlying clusters and diverse geographic locations. This level of redundancy provides a high performance and highly available system that can dynamically expand to meet the customer's needs. When a customer or application needs to gain access to data the Machine Access Control list system is called and based on authorisation can reconstruct the shards and grant the encryption key necessary to recall the data. This ACL system includes both server level as well as user level access. All of this is an abstraction from the GCP experience which ensures that GCP users cannot gain access to the underlying distributed file system, Machine ACL or architecture.

Google encrypts data as it is written to disk with a unique combination of per-shared encryption key and per end-user (ACL) permissions. This architecture is used to break large sets of data into smaller pieces that can be divided among many servers and allows petabytes of data and stores data in a low-level storage system composed of commodity disks.

Replication

Regional (known as Replicated) Persistent Disk (RePD) provides durable storage and synchronous replication between two zones in a region. The two replicas of a RePD are created in separate zones, allowing disks to failover without data loss. This means users are not required to replicate their persistent data across different zones in a region in order to achieve quick failover in case of a single zone failure.

Snapshot

Standard Persistent Disk snapshots use Google Cloud Storage as the underlying storage. A user can use the snapshots to make a backup of a persistent disk at a point in time. Snapshots can be used to make a custom base image or create a virtual machine. Each

snapshot is incremental and will; only contain changes since the previous snapshot; snapshots are geo-replicated and be restored in all regions by default.

4.2.6 Data Deprovisioning and Disposal

Google carries out a rigorous sanitisation process prior to the disposal of media, when released outside of organisational control or released for re-use. In the event media needs to leave Google premises the media is subject to a thorough data sanitisation process carried out by suitably qualified and cleared Google technicians. Media sanitisation follows a clear and purge method as recommended by NIST SP 800-88, These erase results are logged and tracked by the media's serial number and part number. There is a secondary check before the media leaves the secure facility to ensure the records indicate the media has been sanitised.

Google Workspace provides for users a range of options for data deprovisioning to help organisations manage departing users' data securely. Here is an overview of how to handle data deprovisioning in Google Workspace:

- Reassign Ownership of Google Drive and Gmail Data
  - Google Drive: Before deleting an account, you can transfer ownership of Google Drive files to another user in the admin console.
  - Gmail: Email data can also be transferred, ensuring that important emails are retained.
- Use Google Vault (If Available)
  - Google Vault allows you to archive data for legal or compliance purposes. You can set retention rules and place legal holds on users' data to retain it after their accounts are deactivated.
  - Vault is ideal if you need to retain access to emails, Drive files, or other Workspace data after an account is deleted.
- Download or Export Data with Google Takeout or Data Export Tool
  - Google Takeout: Individual users can export their data (such as Drive files, Gmail, Calendar, etc.) before leaving. This is useful for employees leaving on amicable terms.
  - Data Export Tool: Admins can use the Data Export Tool to export an entire user's data before deactivation. This provides a complete backup of a user's account.
- Suspend Accounts Instead of Deleting
  - Suspending accounts rather than deleting them retains all data, however the user cannot access it. This is a good option if you're unsure about deleting the data immediately.
- Service-Specific Deprovisioning
  - For certain Workspace services, users may need to deprovision data separately. For example, Google Chat history or Calendar events might need specific attention based on organisational needs.

These options help ensure that data is retained, reassigned, or properly archived, and assists organisations stay compliant with policies and regulations during offboarding.

4.2.7 Supply Chain Risk Management

Google's supply chain risk management program covers risk identification, assessment, evaluation and risk treatment. Through defined processes procurement teams can manage

Google's supply chain and are able to identify and track external risks to the organisation and its assets such as natural disasters, civil disobedience, labour uncertainty and security compliance concerns.

Whilst Google conducts virtually all data processing activities, Google may wish to engage third parties to provide services. Prior to onboarding third party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide an appropriate level commensurate with the service they provide.

The Vendor Security Audit team reviews the security practices of vendors and the security posture of their products or service against Google's security requirements. Vendor security audits are required for any Google team that is considering contracting with a vendor that will provide a service that Googlers or customers will authenticate to, when the vendor will be in direct contact with Google customers (i.e. on the phone, mail etc), and when Google will be sharing and of the following with the prospective vendor (or the vendor collects for Google):

- User data, Customer or Google PII
- Sensitive Google financial or legal data
- Any other information which, if leaked could result in monetary or reputational damage to Google
- The vendor will be accessing a Google internal service where any of the previous conditions exist

The assessment consists of a vendor questionnaire, documents review and a hands-on-nonintrusive black box assessment. As a result of the assessment the Vendor Security Audit team will document a written assessment of the vendor's entire security program as it applies to the product or service Google is considering. The written assessment details the issues found, the associated risks and recommendations for addressing the risk.

All vendors are required to sign non-disclosure agreements and confidentiality agreements, these documents inform the vendors of their responsibilities to protecting Google Data and trade secrets. Vendors that support the manufacturing, inventory, logistics and disposal services within Google supply chain go through an assessment at least annually to verify minimum baseline security requirements issued by Google are met.

4.2.8 Vulnerability Management

Within Google a dedicated team exists, The Vulnerability Intelligence team is tasked with managing vulnerabilities for servers, the network, applications and third-party software. The vulnerability intelligence team identifies vulnerabilities from many sources including scams of internal and external infrastructure, vulnerability alerts and monitoring, external penetration tests and internal flaw identification software.

Due to the size of Google and its infrastructure quarterly internal and external scans are undertaken on a core sample of production infrastructure, these scans whilst do not satisfy the ISM controls do satisfy requirements from multiple other compliance programs such as FedRAMP and PCI. Google performs further analysis on vulnerabilities identified in scans and files bugs as appropriate to notify teams of remediation items.

Google performs several periodic penetration tests of the Google external perimeter; these tests are undertaken by third-party contractors and completed at least annually. The Google

meirad@botmaker.io

orange team also performs penetration tests to identify system vulnerabilities throughout the Google environment. Security engineers analyse the results of the Google and third-party performed penetration tests, and valid bugs are risk rated and ranked for tracking and remediation.

Google performs on-going internal flaw remediation and identifies application vulnerabilities using a suite of tools that are designed to identify vulnerabilities such as cross-site scripting (XSS) that potentially could be exploited in Google applications, Further tools are used to detect and analyse unsuccessful attempts to perform attacks to obtain intelligence on what products are attractive to attackers, and search for attack signatures in application logs to identify potentially malicious behaviour. Google has a Vulnerability Reward Program [9] that encourages the external research community and other individuals to identify and privately disclose security bugs in Google applications. If the bug is of appropriate severity, the bug reporter receives a cash reward. The scope of the program includes all web properties. There is a 24/7 on-call rotation to monitor the receipt of these reports, and each issue is triaged by a security engineer and valid bugs filed on Google's bug tracking system to be tracked to remediation.

Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement.

bernard@barrken.io

4.2.9 Incident Response

Incident Management at Google (IMAG) is a program developed to provide a consistent approach for the Incident Management teams to handle all types of incidents and provides an organised and effective approach. The goals of the IMAG framework are broken down into 3Cs:

- Help **Coordinate** response effort
- Ensure **Communication** between responders, and the outside world
- Keep **Control** over the incident response

When an incident is declared the responders follow the IMAG protocol to organise themselves in a pyramid structure, with the Incident Commander (IC) at the top. Roles for Incident Management are clearly defined:

- Incident Commander: The Incident Commander is responsible for coordinating the response and delegating key responsibilities.
- Operations Lead: Manages the technical investigations, mitigation and remediation efforts.
- Legal Lead: Ensures compliance with legal obligations, including customer notifications.

[9] https://bughunters.google.com/

- Product Lead: Makes high-level decisions particularly around resource allocation.
- Communications Lead: Drafts and manages internal and external communications.

Communication during an incident is critical and miscommunication can lead to serious mistakes as such the IMAG program provides well defined and documented communication principles for the Incident Management team to follow.

Incident Management team prepares, tests and maintains the incident response plans and escalation procedures, The team conduct regular incident response training and exercises to test the incident response capabilities. The Incident response team incorporates lessons learnt from such exercises or real-life incidents by writing post-mortems. These lessons learned are incorporated into updating response plans or uplifting controls.

Cyber Security Incidents within Google could be categorised in two ways:

- Privacy Incident: Incidents that results in the unauthorised use or disclosure of PII/ PHI
- Security Incident: Incidents that impact the confidentiality and or integrity of a system or user data

Incidents within Google follows in order the Incident Stages:

- Detected: One or more signals have been added to create the incident, but no severity has been set.
- Triaged: Initial triage has been completed, and the severity has been set.
- Mitigated: The incident is no longer impacting users
- Resolved: The incident no longer requires active incident response
- Documented: The incident has a postmortem in progress so relevant teams can improve and learn from this incident.

For impacted customer services, Google provides up to date public notifications for Google Services [10] and Workspace.[11]

bernard@botmaker.io

4.2.10 System Development Lifecycle

Google has implemented a software engineering framework with a core set of principles that are implemented by application development teams that includes coding standards and assignment of security responsibilities. All changes to the information systems follow the SDLC process.

The formal SDLC process kicks off when a code file from the proprietary version control system called Piper is checked out and saved as a local copy for a developer to work on in the Integrated Development Environment. After the developer finishes making changes, the code file is checked back into Piper where a change list is created, and a code review would be conducted and tracked in Google's Proprietary Release Management Tool called Critique.

The author of the file cannot be the reviewer of the file in order to create separation of duties. Additionally, ownership of sensitive configuration files is assigned to security teams to

[10] https://status.cloud.google.com

[11] https://www.google.com/appsstatus/dashboard/incidents/qjmcFHHibfBDsxAjhFnU

ensure that they are involved in the decision-making process to implement developer changes to files that they own. After the file is reviewed and approved it is pushed into the tool Tap where the change code file is compiled for pre-submit testing including unit, regression and system tests. If all tests are passed it is then pushed to a tool called Rapid where a release candidate is created from the change and deployed into a subset of production that is isolated from the rest of the production traffic by using load balancing to ensure customer traffic is not susceptible to potentially negative effects of the change. After passing this stage the build is signed and released.

This development process is adhered to across all of Google from the top of the application stack down to the Kernel and firmware. Google as an IaaS and PaaS provider uses and develops mobile code in support of their business operations. Google performs ongoing assessments of mobile code to determine their risks. Security is incorporated throughout the coding process and the use of mobile code is restricted when deemed to present a security risk.

All user interfaces are designed with secure coding practices to prevent web attacks such as cross site scripting or other popular input-based attacks. If a user attempts to input data that does not meet system parameters, the system will reject the input.

4.2.11 Support Model

Google's Site reliability engineers (SREs) teams are distributed globally and split up across multiple offices, this ensures that on-call staff for the production services can fit into each site's working hours. All engineering and operations teams at Google have escalation ladders, an escalation ladder describes the on-call calendar for a service of which has several components:

- An interval-list specifying how much time to spend on each escalation level (i.e., if the first on-call doesn't respond, how long to wait before notifying the next on-call.
- A start time that specifies the on-call starting time of all contacts on the contact list.

The on-call engineers for each product oversee responding appropriately to pages or alerts, The on-call shifts are distributed among engineers in the same team, to support one or several services.

- Primary Responder: The primary responder is the person driving the response of the incident. That is pursuing a mitigation and updating the incident with key findings and periodic summaries.
- Secondary Responder: If necessary, additional personnel to help the primary responder on a non-escalated incident. If additional help is needed, escalating the incident via an OMG ticket raises the profile and awareness of the situation.

For Google Workspace users, support offers several levels of assistance, depending on the subscription type and the urgency of the issue. Here's a rundown of the support options available:

- Google Workspace Admin Help Centre
- Self-Help Resources: The Help Centre provides extensive articles, guides, and troubleshooting steps for common Google Workspace issues, including admin controls, security, app usage, and more.

bernard@hotmail.it

- Community Forums: Admins can ask questions in the Google Workspace Community Forum to get help from other users or Google product experts.
- Google Workspace Support Plans

Google offers different levels of support depending on the Google Workspace subscription:

- Standard Support (All Google Workspace Editions): Includes 24/7 assistance via email, chat, and phone for critical issues (such as service disruptions).
- Enhanced Support (Paid Upgrade): Includes all Standard Support benefits plus faster response times and a Technical Account Manager (TAM) for proactive assistance. Enhanced Support is recommended for businesses that need additional help managing more complex environments.
- Premium Support (Paid Upgrade): Includes all Enhanced Support features and offers the fastest response times, a dedicated TAM, customized technical solutions, and access to Google's Customer Care Portal.
- Contacting Google Workspace Support

Admins can contact Google Workspace Support in the following ways:

- Admin Console: Go to the Admin Console, navigate to Support > Contact Support for phone, email, or chat options.
- Phone Support: Google provides direct phone support for admins, which you can find under Support in the Admin Console.
- Chat Support: For quick questions, chat support is available directly from the Admin Console.

Priority and Severity Levels associated with the service:

- When contacting support, admins can indicate the severity level of the issue (ranging from P1 - Critical, to P4 - Low). The response times vary by the support plan and severity level, with Premium Support offering the quickest responses for high-priority issues.

Google Cloud Support Portal to file and manage support cases for your organization:

- Customers on Enhanced and Premium Support plans can access the Google Cloud Support Portal, where they can track issues, communicate with support engineers, and monitor case statuses.

benedikt@stackone.com

4.3 Administrative and Support Environment

4.3.1 Administrative and Support System Overview

Access to production resources requires users to have a valid certificate. To obtain the certificate a user is required to use a Google managed production based workstation. The users are required to supply a username, password, and second factor authentication using their single-factor cryptographic device. The certificate that provides access to the production environment is valid for no more than one day, ensuring that an account that is inactive for more than one day will not be able to access the production environment. Device access within the production network requires each device to have a valid machine certificate installed. The certificate that provides access to the production network only establishes the device's identity, and the device is authenticated each time it tries to gain access and at a minimum, once per day.

The Google Security Team requires devices to be configured to lock or close sessions after 20 minutes or for users to lock or close sessions when the device is unattended.

In addition, Google has enabled session locks on end user production based workstations in the form of a password-protected screen-saver that activates after 15 minutes of inactivity. The screen-saver remains locked until the user signs back into the computer. Google security policies require employees to safeguard their production based workstations if left unattended for any amount of time and supports this requirement with Data Security Guidelines and production based workstations security training.

The Google Security Team restricts all Google user access to the production environment to Google managed hardware. Access to the production environment is only allowed from the Google corporate network. In order to authenticate to the Google corporate network, Google laptops and workstations require a valid machine certificate, ensuring that only Google managed devices can connect.

The Google Security Team also temporarily limits the access of Google users if they travel to certain restricted countries. When a Google user returns from a restricted country they are required to take action to remove the restriction from their account.

bernard@brinkr.io

4.3.2 Physical Security

During the assessment the assessor visited two datacentres and completed interviews and inspections with the relevant datacentre staff and Google staff onsite.

For the Australian regions of Google Cloud Platform, Google Workspace and GCVE colocation is utilised within Datacentres located in two major cities with geographic separation. Infrastructure and staff are provided dedicated areas including office spaces and data halls that ensure complete segregation and the ability to apply and manage their own access controls on top of what is provided as part of the colocation agreement for the facility. Data Halls within respective datacenters are rated to SCEC Zone-3 area within a compliant Zone-2 shell..

Access to the data halls require security verification in accordance with the site specific security management plan which includes:

- Site boundary perimeter
- 24x7 manned security office and personnel checkpoint
- NSW Health directive screening

- Perimeter vehicular security checkpoints in the form of unrated security gates
- CCTV monitoring and capture of perimeter and internal access by digital cameras
- Biometric and proximity card access points to data hall and other secure areas
- 24x7 access permitted to authorised personnel

Access to datacentre common areas is managed by facility staff, requiring a valid reason and point of contact to enter the grounds of the facility and the security booth. Upon visit government issued photo identification is required and induction to the facilities emergency response procedures. It was evidenced to the assessor that appropriate video surveillance was in place with robust procedures to ensure that whilst footage is recorded and maintained, security personnel can always maintain visibility of the video walls with staff rotations.

Specific facility access cards are provided which allow the assigned access to locations within the facility, however these cards do not provide access to Google spaces as their access controls are managed separately. Visitors to Google spaces require Google staff to raise access requests prior to site visit; this is completed through the facilities Data Centre Visitor Management System and requires a valid justification. To access Google managed colocation spaces a separate card is required as they function their own access control systems, likewise the security surveillance systems are independent to the facilities and managed by Google SOC (GSOC). The GSOC team has the ability to correlate audit record analysis with physical access monitoring in order to enhance their ability to identify malevolent activity within the Google Services environment. The GSOC has the ability to view camera footage at each of its data centers to investigate physical security incidents. Similar to its audit review processes, Google will notify the proper authorities once an event is determined to be an incident at any of its facilities. Data Hall access is controlled by two factors of authentication dependent on the location for Google Cloud Platform data hall access: a swipe card and retina scan is required, for Google Cloud VMware Engine data halls a swipe card and pin. Entry and exit points of the data halls are physically manned and upon exit a minimum of two security personnel complete a body scan to ensure no metal objects are removed.

Within Google spaces a class 5 intruder alarm is installed and monitored, furthermore laser curtains are armed out of hours ensuring access through walls and ceiling will be detected. VESDA smoke detectors are used throughout the facility to ensure incidents are picked up early by facility staff.

4.3.3 Segmentation and Segregation

Within GCI resources are shared to perform multiple purposes, as such Google is focused on logical protections and separations to protect against unauthorised access. Security in the system environment managed by Google is shifted from the system boundary to the device level. Communications at the external managed interfaces and at key boundaries are monitored and controlled. Google owns and operates the networking equipment from the peering on the network edge down to the datacentres. The fiber connecting the data centres is operated by Google.

User functions on systems and devices supporting the Google products are separated from administrative or system management functions via a layered approach consisting of account authorisation and logical access restrictions. Administrative functions require the use of Google equipment that requires valid machine certificates for Single Sign-On

authorisation and requires a username, password and 2FA token to access the production environment. Access to production machines and networking devices is further secured through machine ACL's and network Authentication, authorization, and accounting (AAA) service access permissions.

Traffic between the corporate environment and the production environment is controlled by routers and monitored by the Network operations team. Machines within the production environment cannot establish connections to the internet, unless specific business justification and authorisation has been sought and approved in which case designated proxies are utilised.

Google uses Software-Defined Networking (SDN) to segment portions of the network for performance and process isolation, including security and support components. The SDN results in a logical separation from the internal networks. Connections to and from these isolated networks are controlled with (ACLs).

bernard@photmaker.io

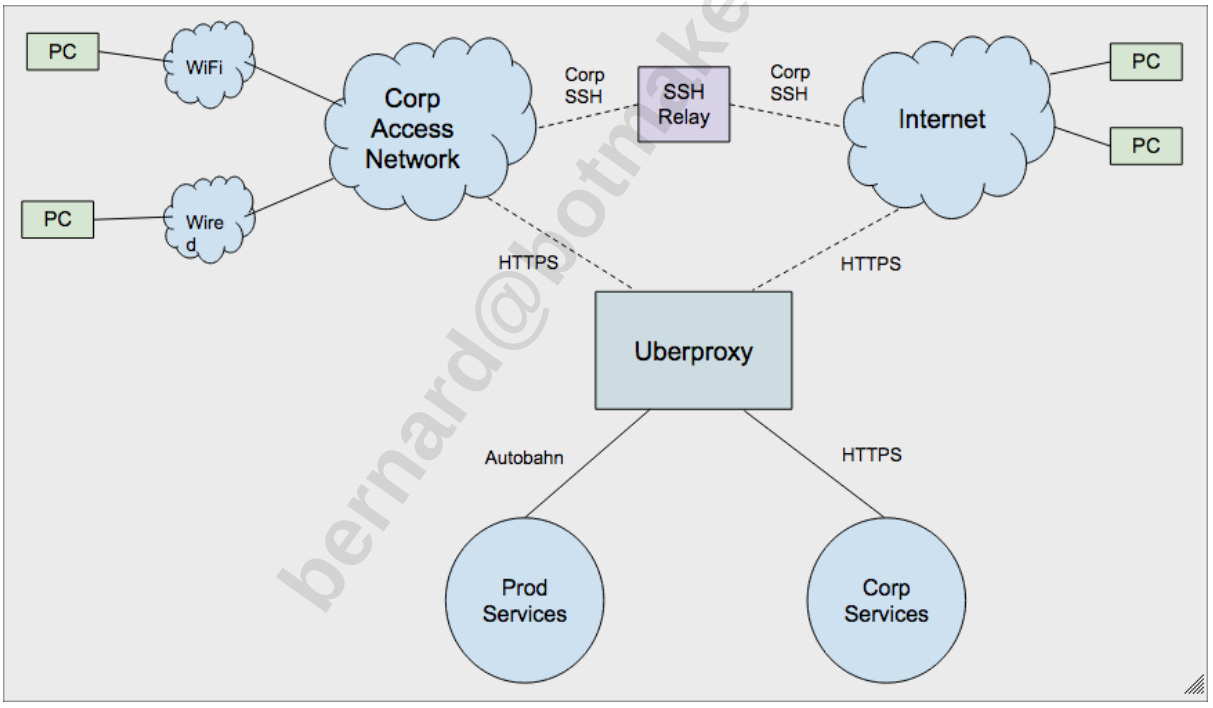


Figure 6: Separation between Production and Corporate Environments

4.3.4 System Hardening

The Security team monitors and audits deviations from the machine baseline configuration on a daily basis, In the event that an unauthorised change to software, firmware and information are detected, stakeholders are notified to review, and the system automatically attempts to restore an authorised software state, if this attempt fails then stakeholders are notified further, and the system is re-imaged. Production devices are not equipped with USB ports or CD/DVD drives which further limits where unauthorized code could be introduced to the environment.

Google's proprietary hardening implements industry best practices to protect memory from unauthorized code executions, such as prohibiting the execution of code in non-executable regions of memory or in memory locations that are prohibited. Google utilises 64-bit

processes within the production environment that contains hardware Memory Management Unit (MMU) to provide virtual address space technologies. This, in conjunction with OS support, restricts each application's access to only memory assigned to the application.

Google uses various isolation and sandboxing techniques for protecting a service from another service running on the same machine. These techniques include normal Linux user separation, language and kernel-based sandboxes, and hardware virtualisation. As an extra security boundary Google enables very sensitive services such as the cluster orchestration service and some key management services to run exclusively on dedicated machines.

MSV (Machine State Verification) is the system that synchronizes firmware/bios images and system files on the root partition across the vast majority of production machines. MSV is part of the node software ecosystem. Configuration policies are specified in Piper and file content is provided by a set of Midas packages of known provenance. The same configuration and content are also used when installing new machines.

The Assimilator team manages MSV, a suite of applications and infrastructure used to implement and oversee standard machine images across Google's Production network. Production security hinges on effective image, package, and critical binary management. Image file checksums are used to prevent tampering. A periodic pusher job ensures the accurate distribution of golden images to production. Detected changes (to the machine or configuration files) trigger a corrective process: the base image is copied back to the machine's root partition, and any extraneous elements are removed. All MSV changes are logged.

4.3.5 Secure Administration

To access the production environment the users first identify against the Single Sign-on service which prompts for username, password and 2FA to obtain the required certificate for SSH, this certificate is valid for less than one day. The certificate obtained allows the user to authenticate to machine resources which then uses the machine ACL system as the authorisation system of record and networking devices using the Network AAA service as the system of record. Google does not permit remote connections into the production environment from any non-Google managed workstations or laptops, The only path to the production environment is through the Single Sign-On service.

Google uses a number of encrypted mechanisms to protect the authenticity of connections used in the management of the production infrastructure these include:

- Secure Shell (SSH): Authorised Google personnel use SSH to connect to production resources.
- Proprietary transport security protocol similar to mTLS: Used for service-to-service connections within the Google network

All traffic between data centres is encrypted using a FIPS 140-2 or FIPS 140-3 validated solution.

The Google Security Team restricts all Google user access to the production environment to Google managed hardware. Access to the production environment is only allowed from the Google corporate network. In order to authenticate to the Google corporate network, Google laptops and workstations require a valid machine certificate, ensuring that only Google managed devices can connect.

h.rand@bothrayer.ro

The Google Security Team also temporarily limits the access of Google users if they travel to certain restricted countries.

Google has announced the implementation of the BeyondCorp initiative to rethink how to secure internal applications and services and the definition of the security perimeter. Google has transitioned to a new security model that dispenses with a privileged corporate network. Instead, using the BeyondCorp methodology, access depends solely on device and user credentials (ACLs), regardless of a user's network location. As a result, all Google employees can work successfully from any network, and without the need for a traditional VPN connection into the privileged network.

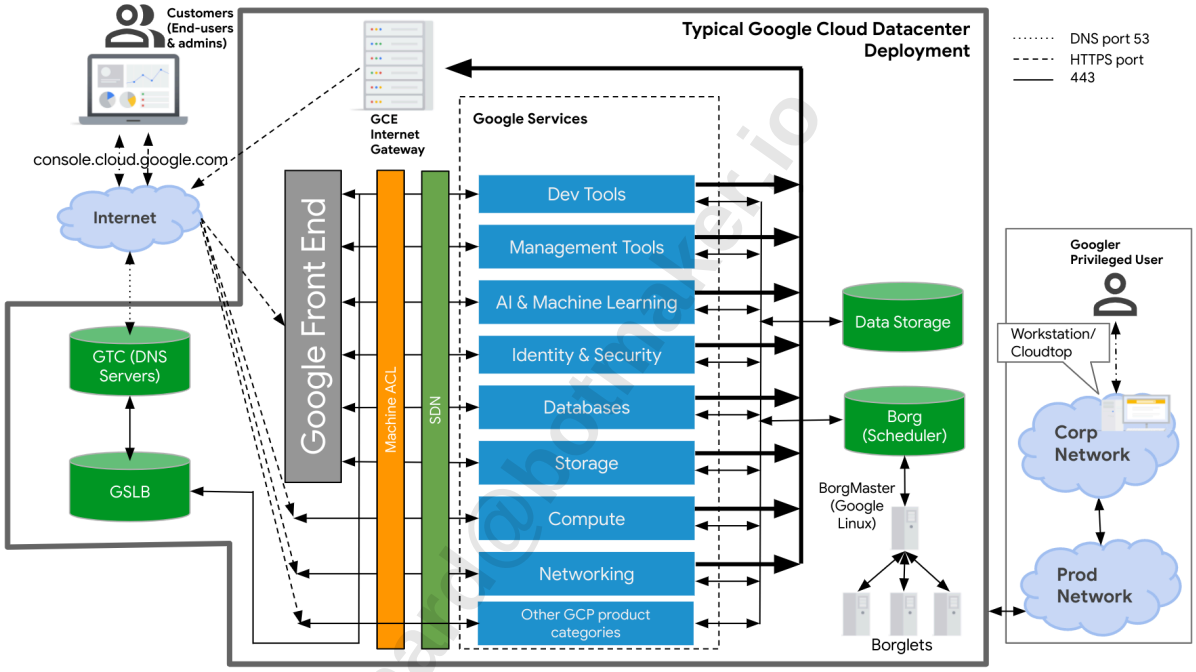


Figure 7: Access paths to the production environment

bernard@hotmail.io

4.4 CSP's Cloud Protection Environment

4.4.1 Network Security

The Google production network is connected to the Internet through multiple peering points and routes to this network are advertised through Border Gateway Protocol (BGP) as a public autonomous system. Google manages the fibre optic network that connects the data centres. Traffic is routed to Google Front End (GFE) machines that provide load balancing between machine clusters and directs traffic to application services.

Google production systems use a proprietary non-DNS based address resolution service for internal traffic to authenticate the origin and verify the integrity of messages, The Global Traffic Control (GTC) is the external traffic balancer for Google, It uses the Domain Name System (DNS) protocol to direct service requests to a data centre for the service that is available and spreads network load across data centres in a geographic region, sending excess load to other regions. Load balancers handle the address translation and are configured with the public-facing IP addresses used by Google.

At the data centres, Google uses commercial and proprietary hardware equipment to connect to the backbone, redundant interconnected routers provide high availability connectivity. Connections between internal Google resources use a proprietary service similar to Remote Procedure Calls (RPC) that provide peer-to-peer authentication similar to Kerberos. All traffic is at least cryptographically authenticated between machines, while some connections including to and from the Key Management Service are encrypted using Google's proprietary service similar to SSL and Kerberos using BoringCrypto.

4.4.2 Decommissioning Hardware

Google carries out a rigorous sanitisation process prior to the disposal of media, when released outside of organisational control or for re-use. In the event media needs to leave Google premises the media is subject to a thorough data sanitisation process carried out by suitably qualified and cleared Google technicians. Media sanitisation follows a clear and purge method as recommended by NIST SP 800-88, These erase results are logged and tracked by the media's serial number and part number. There is a secondary check before the media leaves the secure facility to ensure the records indicate the media has been sanitised.

Media that cannot be sanitised is destroyed by physical destruction methods described in NIST SP-800-88 Rev. 1, This destruction is carried out within Google's dedicated data halls by appropriately qualified and cleared Google technicians.

Outsourcing the destruction to third-party vendors is permitted, However, these vendors are obligated under contract to abide by Google's guidelines for data destruction. When third parties are engaged then the processes they undertake are audited including both transportation and destruction processes through the use of the Vendor Security Assessment.

Equipment such as spares are stored within the Pharmacy located in the Google dedicated data halls.

bernard@brinkwire.io

4.4.3 Security Operations and Monitoring

There are many different teams within Google who support various security and privacy incident responses. Their combined mission is to Protect, Respect and Defend Users, Googlers and the Internet.

- Detection - Security Surveillance Team (SST)
    - The SST investigates aggregate signals and works closely with the Incident Management (IM) team and Threat Analysis Group (TAG) to determine the validity and severity of issues. The SST resolves low to medium-severity threats; escalates higher severity threats to their counterpart teams.
- Detection - Insider Threat Detection Team (ITF)
    - The Insider Threat Detection team investigates suspicious activity related to insider threats and works closely with partners around the company to verify validity and severity of issues.
- Incident Management (IM)
    - The Incident Management team manages the critical privacy and security incidents, partnering with teams throughout the company to perform impact and scope analysis, remediate incidents and assist with the design of long-term solutions. The team operates from three sites allowing for 24x7 coverage with a response SLO of 30 minutes or less.
- Privacy Incident Management (PIM)
    - The Privacy Incident Management team improves Google's privacy posture by effectively managing, analysing and preventing privacy incidents. The team is based in two locations and manages incidents of P1 or lower. The PIM team carries a response SLO of 60 minutes or less on business days.
- Apps Incident Management (AIM)
    - The AIM team manages incidents related to systemic Trust (Privacy, Security, Data Loss & Media) issues impacting Workspace products. The AIM team is global and 24x7 on call team.
- Cloud Incident Communications (CIC)
    - The CIC team delivers best in class Incident Communications for all Cloud products with full compliance with regulatory and contractual obligations.
- Digital Forensics (DF)
    - The digital forensics team works closely with Incident Management and SST to investigate the scope and impact of incidents. The DF team performs digital forensics and provides technical expertise for investigations into employee misconduct.
- Vulnerability Coordination Centre (VulnCC)
    - The Vulnerability Coordination Centre – VulnCC team ensures that Google has a consistent, well-functioning process for vulnerability management across the entire organisation., and coordinates complex, high severity or sensitive issues.

bernard@bonmaker.io

- Threat Analysis Group (TAG)
  - The Threat Analysis Group provides malware reverse engineering support, special in-depth investigative services, ongoing penetration testing and situational analysis to Google's Security Teams and Google Management. TAG protects both Google and Google users against targeted attacks by producing and disseminating threat intelligence while developing tooling to respond to new threats at scale.
- Cloud TF
  - Cloud TF is part of SST and mainly focused on developing and establishing effective monitoring and detection capabilities of Google's Cloud Environment (GCP) for threats to Google's-owned projects.

4.4.4 Cryptography and Key Management

Google effectively establishes and manages cryptographic keys in accordance with Google-Specific practices. Google follows formal practices for key generation, distribution, storage, access and destruction that are informed by industry best practices and NIST SP 800-57 – Recommended for Key Management. Google establishes and manages the certificates used for Internal communications this is achieved using Google's Certificate Authority to sign all certificates. Google uses a proprietary key management service to manage the generation, distribution, storage, access, rotation and destruction of cryptographic keys.

The Key Management service is hosted on a custom-designed operating system based on a stripped-down hardened version of Linux. The homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard Google image, the system is automatically returned to its official state. Google uses a proprietary system to periodically generate and rotate an encryption key used to protect user data at rest. The system helps ensure that key customer data is not encrypted with a discarded key.

Google protects the integrity of transmitted information by only accepting traffic that conforms to the specification of the network flow policies and by using reliable protocols with error correction to transmit information. External authentication between the user's web browser and Google uses TLS/SSL encryption when users authenticate to their domain and for the life of the session. Customer core content is encrypted between customer clients and Google, between Google data centres and at rest. The Security Team requires the use of strong encryption throughout the environment, Google uses FIPS-140-2 Level 1 overall with Level 3 physical security certified Titan keys as the second factor authentication for Google users with administrative rights to Google Cloud Platform and its underlying infrastructure.

bernard@bernard.io

4.4.5 Data Transfers

Google stores customer core content data at rest in regional data centers, based on the geographic location of the customer's primary domain name. For customers with a primary domain name located in Australia, core content data is stored at rest in Australian data centers. Customer core content data is encrypted between customer clients and Google, between Google data centers, and at rest. Encryption between an agency customer and Google servers is dependent on the customer's client configuration.

4.4.6 Identity and Access Management

At the core of Google's identity management is Ganpati, Ganpati is the canonical service for user, group and membership management for both the corporate and production environments. The users and groups within Ganpati are structured in parent/child relationships where the group itself is called the parent and the member user is called the child. A user or group can be the child of multiple different groups, so it can have multiple parents.

A user is identified by their username and namespace known as a Gaia ID, when users are provisioned accounts, they are given two Gaia ID's, such as "user.corp" and "user.prod". All changes made to Ganpati data happen via proposals, A proposal is a change request and is approved before it can be implemented. Once approved, the change described by the proposal is applied to the Ganpati datastore.

Ganpati has the concept of roles, a role is used for assigning permissions within Ganpati and can be defined as one of the following 3, Owner, Leader or Proposer.

- Owners can approve proposals that add, change or remove children from that group, AND approve proposals that add, change or remove owners or leaders from that group AND approve.
- Leaders can approve proposals that add, change or remove children from that group.
- Proposers can propose membership changes however cannot approve them.

When a role is granted to a group, all descendants of that group also have the permissions of that role. Multiple roles for a group may be either directly or indirectly granted to a user/ group. Google limits group membership based on job responsibilities and least privilege, furthermore memberships to groups with access to production environment resources requires users to have the necessary technical background, training and understanding to assume permissions associated with the group membership and have completed the appropriate and relevant security and role-based training.

Conditions for group membership are determined by each resource owner(s) and requests for group membership are individually reviewed and approved by the resource owner(s). Further to the users and groups listed previously the Google Security team has identified two additional types of accounts to support Google Services, Machine ACL accounts and Network Administrator accounts, Google do not provision Guest, anonymous or temporary accounts.

- Machine ACL accounts are defined as a record within the Machine ACL system that includes a username and group membership.

bernard@lotmaker.io

- Network Administrator accounts are created for users with responsibilities to manage network devices, Access to the production environment network devices is managed by the network AAA service.

The Google Security Team uses the Google Human Resource system to align account management processes with personnel termination and transfer processes. The Human Resource system provides automated workflows for the creation and separation of employees including temporary, vendor and contract employees. This system syncs with other user databases, providing an automated workflow to create and disable user accounts based on actions within the Human Resources System. Human Resources or Resource Owners revoke privileged access when the access is no longer appropriate. This includes revoking access for a user when:

- Access is no longer required to perform their assigned job duties
- An employee no longer works at Google

Timeliness of revocation of privileged access is escalated depending on the sensitivity of the specific privileges and the nature of the access termination (e.g., user is on leave, user termination). If necessary, privileged access for a user can be revoked expeditiously based on severity.

The Google Security Team uses the Machine ACL system to track and monitor privileged access assignments. Membership in Machine ACL groups with access to production resources is considered privileged, and as such are periodically reviewed by the corresponding resource owner(s).

bernard@bornaker.io

4.4.7 Security Automation

Due to the size, scale and complexity of Google and its associated products and infrastructure automation sits at the core of most tasks within, Google limits the usage of commercial off the shelf solutions instead opting to build proprietary systems.

Google's security team continuously monitors log activity in the production environment by creating and modifying alerts. A proprietary event management tool automatically analyzes and prioritizes alerts based on severity, flagging them for manual review by incident analysts. These analysts then notify the appropriate security and organizational personnel if they find evidence of valid suspicious activity. The event management tool's automated analysis and integration with organizational processes enable efficient investigation and response to potential security threats. Once an event is identified, it enters a queue for human review, which is managed by a 24/7 team. Google also audits specific events deemed relevant to the environment's security posture, integrating these findings into incident response, continuous monitoring, and contingency planning processes.

The Google Security Team utilizes automated analytics to monitor logs for suspicious activity and generates alerts when it is detected. Examples of suspicious activity include users logging in from unexpected locations and a user accessing resources from outside the local domain. Google has a vulnerability management process that identifies vulnerabilities during Continuous Monitoring. Google Security Team uses proprietary audit tools and other automated capabilities to identify and investigate such vulnerabilities.

New Google employees (including vendors, contractors, and temporary employees) are assigned Google accounts on their first day of employment. techstop selects a username to uniquely identify an individual as part of the onboarding process managed by PeopleOps.

During the account setup process an automated workflow checks with the identifier repository to verify the uniqueness of the identifier. When an employee is terminated, upon the determination of a termination date of a Google employee, the Google Exit process is initiated. Each departing employee is assigned an HR Business Partner (HRBP) who is responsible for inputting the exit workflow information into the human resources database. The exit workflow includes automated notification to the Asset Recovery Team to recover assets assigned to the terminating employee. The Google Security Team uses automated methods to limit remote connections to the production environment to Google machines with a valid machine certificate.

4.4.8 Continuity and Availability

Google assumes no loss or downtime is acceptable to end-users and has designed a highly redundant architecture from the ground up-aimed to achieve high availability. Google does not perform traditional contingency planning and therefore does not conduct a traditional information system-wide business impact analysis to determine the Maximum Tolerable Downtime or acceptable data loss. Google has established an internal service level agreement framework between infrastructure teams and internal customers that set performance metrics between 99% and 99.95% depending on the service. This very high level of availability dictates an aggregate Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of near zero.

Within Google DiRT, or Disaster Recovery Testing is a program to enable continuous and automated disaster readiness, response, and recovery of Google's business. Systems, and data. DiRT sponsors events throughout the year as part of the ongoing efforts around response and recovery and provides guidance and education.

Google takes a layered approach to Denial-of-Service (DoS) mitigation to ensure continued availability; this includes control points within network routers, network load balancers, application load balancers, and the application design. In most cases the goal is to mitigate impact, so techniques often use throttling to a level that can safely be absorbed by Google's global infrastructure, thereby also minimizing collateral damage caused by potential false positives. Google monitors the health of the network and security devices on a 24/7 basis. Incidents which cause impact, or nearly cause impact are thoroughly investigated, Including by DoS experts if warranted. Tactical response actions or escalations for long-term initiatives are taken as appropriate.

sekuro Confidential

5 Assessment of Cloud Services

5.1 Cloud Service Assessment and Consumer Guidance

The IRAP assessment conducted was an independent evaluation of the implementation, appropriateness, and effectiveness of a system's security controls. The results of the IRAP assessment have been documented in this security assessment report. This report is used by consumers to assess and authorise a system's suitability for their security needs and risk appetite. While the approach taken to conduct an IRAP assessment depends on the size and complexity of a system, there are foundational assessment stages and principles that have been applied to each phase of the assessment.

During the Google cloud security assessment, the IRAP assessor incorporated the guidance from this document to ensure that the IRAP assessment and in-scope Cloud Controls Matrix (CCM) controls met their objectives and the expectations of the consumers of security assessment reports.

For further details on the Consumer Guidance, please refer to the CCM attached in Appendix A of this report.

Document Watermarked

4.1.1 Description

Google uses its own Google Cloud Infrastructure (GCI) coupled with Google Cloud Platform as the hosting infrastructure for Google Workspace. Google operates, manages and controls the components from the host operating system and virtualisation layer down to the physical security of the facilities in which Google Cloud Infrastructure hosting Google Workspace operates. Google assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the firewalls. Google retains ownership of the infrastructure (not the user-data stored thereon) while providing services.

Google Cloud Platform (GCP) includes IaaS, PaaS, and SaaS offerings built on Google Common Infrastructure. GCP services range from fully customer-managed virtual infrastructure (IaaS, e.g., Google Compute Engine), allowing customers to provision fundamental computing resources, to CSP-managed platforms (PaaS, e.g., Google Cloud SQL), for deploying applications without managing the underlying infrastructure. GCP also includes system management tools and advanced Machine Learning APIs.

For Google's GCVE likewise Google retains ownership of the infrastructure (but not the user-data stored thereon), whilst also relying on Google to manage the cloud infrastructure including the network, data storage, system resources, data centres, security and reliability.

5.1.2 Cloud Security Shared Responsibility Model

The Google Security Shared Responsibility Model indicates the various layers of responsibility and their respective owners.

Google maintains the responsibility for 'Security of the Cloud', as such, Google is responsible for protecting the infrastructure that runs all the services offered in Google Cloud Platform and Google Workspace. This infrastructure is composed of the hardware, software, networking, and facilities that run Google Cloud Platform and Google Workspace.

Google Cloud Platform and Google Workspace consumers maintain the responsibility of applying the Cloud Security Shared Responsibility Model in their own environment, for example, the consumer is to determine how it applies to their use case i.e., the integration of those services into their IT environment, and the laws and regulations applicable to their organisation and workload. For more detailed information refer to Google's public documentation regarding Shared responsibilities and shared fate on Google Cloud[12].

For further details on the responsibilities of the cloud, see section 5.1 Cloud Service Assessment and Consumer Guidance and Appendix A of this report.

Layer	Responsibility		
	Data Center Provider	Google	Cloud consumer
Governance			
Incident Response	Yes	Yes	No
Backups	No	Yes	Yes
Technical			
Data	No	No	Yes
Identity & access management	Yes	No	Yes
Application	No	Yes	Yes
Platform	No	Yes	No
Virtualisation	No	Yes	No
Physical hosts	No	Yes	No
Physical networking	No	Yes	No
Physical datacentre	Yes	No	No

Table 5: Responsibility Matrix

bernard@botmaker.io

[12] https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

5.1.3 Cloud Service Architecture Diagram

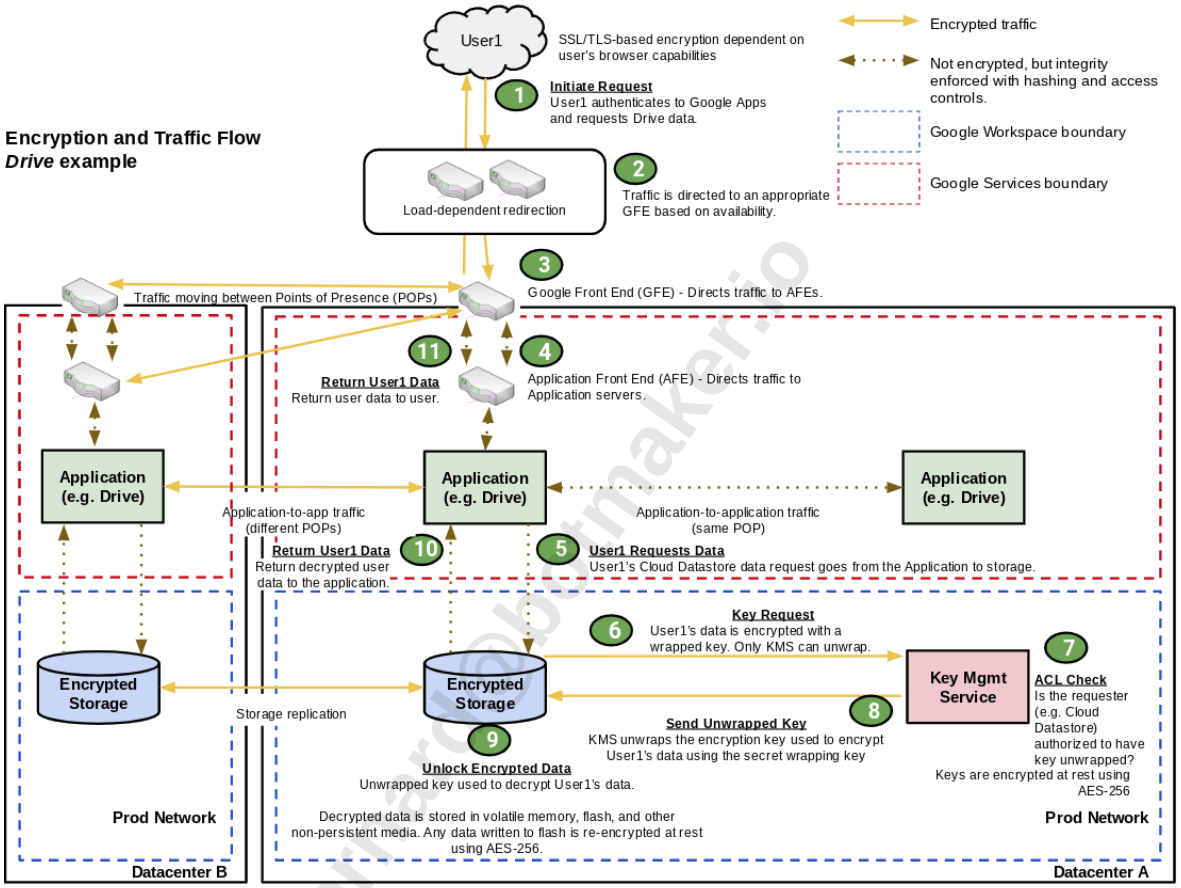


Figure 8: Data flow in and out of the system boundaries

5.1.4 Components and Dependencies

Google Workspace in some instances relies on third-party providers to provide or supply products or services for the enablement of the service as a whole, These are referred to as sub processors and are managed through Google's stringent Vendor Security Assessments and onboarding processes. Sub Processors may be located in various countries across the world and dependent on the service contracted to provide may have access to customer data, only to the extent required to perform the tasks they are contracted to perform.

There are three main types of Sub Processors:

Data Center Operations: Operates and maintains the Google data center and equipment that stores Customer Data. Subprocessor personnel do not require access to Customer Data to perform this activity.

Service Maintenance: Software and systems engineering, maintenance and troubleshooting. In the course of performing this activity the Subprocessor may require limited, authorized access to Customer Data e.g. to remediate technical issues.

Technical Support: Customer-initiated technical support.

For an up to date list of Sub Processors refer to Google Public Document Google Workspace and Cloud Identity Subprocessors.[13]

5.1.5 Inbound and Outbound Interfaces

The Below table outlines the Ports, Protocols and Services which are enforced at the Google Services level for all applications.

Component/ dependencies	Inbound/ outbound	Description
Google Workspace over HTTP / QUIC	80/TCP, 80UDP	HTTP / QUIC
Google Workspace over HTTPS /QUIC	443/TCP, 443/UDP	HTTPS / QUIC
DNS	53/TCP, 53UDP	DNS Traffic
NTP	123/UDP	Alternative source for Google time service
GMAIL	25 TCP, 443TCP,465 TCP, 587 TCP, 993 TCP,995 TCP	GMAIL Email services including SMTP, POP and IMAP.
Google Meet and Google Meet Livestream	3478 UDP, 19302-19309 UDP	WEBRTC for Google Meet
XMPP	5222 TCP	Google Drive (Used only by Backup and Sync client for Mac and Windows)
FCM	5222-5230 TCP	Gmail, Meet, Calendar.

Table 6: Inbound and Outbound Interfaces

bernard@botmaker.io

5.1.6 Protection of Data at Rest

Google transparently encrypts core content data at rest for user-generated data, additionally Google uses BoringCrypto to secure the customer content at rest. Data stored is uniquely labelled and inventoried to allow the file system to identify the location and ownership of the end-user data. Data is not stored in a typical file structure, instead in data “chunks” that are stored on local disks and identified by a unique chunk/ID.

Google uses proprietary service to manage the distribution, generation and rotation of cryptographic keys, files or data structures with user-generated content are encrypted with a key. This key is encrypted by the Key Management Service with a restricted ACL of services allowed to request the Key Management Service to decrypt it. The wrapping keys needed to decrypt user data are only known to the Key Management Service, all access to and from the Key Management Service is controlled via ACLs.

The integrity of data stored in Google’s databases is maintained using data checksums, when a stored file is presented back to the user, the data checksums are used by the distributed file system to ensure each piece of the data presented back is correct. The confidentiality of data is maintained using access controls and unique certificates to ensure that only internal Google support personnel are allowed access to specific data are able to

[13] https://workspace.google.com/terms/subprocessors-20230316/

access it. Google structured databases use an ACL model that maps internal support personnel access rights to which data they have the rights to along with periodic access reviews ensures access remains current and to only what is required.

5.1.7 Data Backup and Restore

Google relies primarily on replication to backup systems and data, therefore, current backups of Google Workspace software and data are shared and replicated across Google Data Centres. Google's production environment is designed to replicate data at multiple locations and the validation of data stored at these locations is automatically and continuously performed by various layers of the data storage systems, which will report any inconsistencies or missing data, and, when possible, automatically restore missing data from another replica. Test procedures have been developed and are used during DiRT to validate recovery directly in the data storage layer from backups.

Google Workspace stores structured data in a vast distributed database built on a distributed file system designed for massive data storage across numerous computers. Data is divided into chunks, replicated across multiple systems to prevent single points of failure, and assigned random, non-human-readable filenames for security. All Google Workspace data is replicated across at least two instances. Additionally, data is often replicated more than two times for redundancy purposes.

Bernard@Bottmarket.io

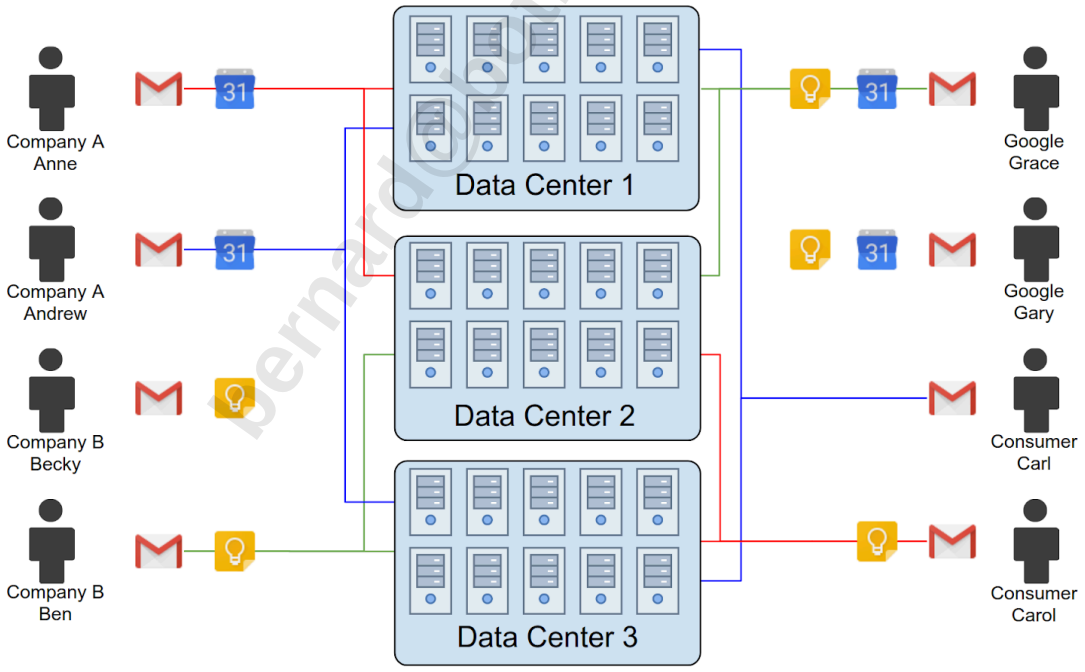


Figure 9: Logical Diagram showing authorisation boundary for assessment

5.1.8 Data Portability

Google Workspace offers users a range of options for data portability to help organizations manage departing users' data securely. Individual users can export their data (such as Drive files, Gmail, Calendar, etc.) before leaving with Google Takeout. This is useful for employees leaving on amicable terms. Admins can use the Data Export Tool to export an entire user's data before deactivation, providing a complete backup of a user's account.

Below are some of the tools provided by Google:

- **Google Takeout:** This tool allows users to export their data from various Google Workspace services, including Gmail, Drive, Calendar, Contacts, and more. It's a good option for users who want to back up their data or transfer it to another service.
- **Data Export Tool:** This tool allows administrators to export data for all users in their organization. It's useful for organizations that need to comply with data retention regulations or want to create a backup of their data.
- **Google Vault:** This tool allows administrators to retain, search, and export user data for legal or compliance purposes. It's a more advanced tool than the Data Export Tool and requires more technical expertise to use.

Before deleting an account, ownership of Google Drive files can be transferred to another user in the admin console. Email data can also be transferred, ensuring that important emails are retained. Google Vault allows for archiving data for legal or compliance purposes, and retention rules and legal holds can be placed on users' data to retain it after their accounts are deactivated. Suspending accounts rather than deleting them retains all data, however the user cannot access it. For certain Workspace services, data may need to be deprovisioned separately. These options help ensure that data is retained, reassigned, or properly archived, and they help organizations stay compliant with policies and regulations during offboarding.

pernard@gotmail.io

5.1.9 Tenancy Segmentation and Segregation

GCI services support two logically separated environments; The Production environment and the corporate environment. The Production environment includes the machines and network devices that supports the public facing cloud offering, Google Workspace. The corporate environment is internal corporate infrastructure systems and services that are used to support Google's internal processes or systems and does not store, process or transmit any customer data.

The Google Common Infrastructure prioritizes logical protections and separations over physical separation into domains or environments due to the shared nature of its resources and their multiple purposes. Services that have resources hosted in GCP leverage technologies like containerization to further isolate the execution of processes and their associated address spaces. This is in addition to the separate execution domains provided by the underlying GCI infrastructure.

Google employs multiple layers of isolation, including standard Linux user separation, language and kernel-based sandboxes, and hardware virtualization, to safeguard services from each other on the same machine. Typically, higher-risk workloads, like running complex file format converters on user-supplied data or user-supplied code, utilize more layers of isolation. For added security, highly sensitive services, such as cluster orchestration and certain key management services, operate exclusively on dedicated machines.

5.1.10 Cloud Service Security Visibility

Google has determined that a continuous automated audit event system and supporting processes are required to monitor and to detect attacks and indicators of potential attacks or compromise as well as any authorised local, network and remote connections.

The Google Security team utilises a distributed deployment model to collect audit log data from Google's servers and network devices, and to centralise indexing to support information searches and audits. Log data is captured locally on devices in syslogs and continuously

sent to proprietary log aggregators. Log data is not lost if connectivity to the aggregator is temporarily disrupted. The log aggregators transform raw data into events and place the results into an index that can be searched using proprietary event management and analytical tools used within Google. Monitoring of the events queue takes place 24 hours per day, 7 days per week.

Communications at the external boundaries and at key internal boundaries are monitored and controlled to prevent unauthorised access or misuse of the systems, furthermore proprietary tools also monitor application logs for exploitation of web application security vulnerabilities. Services with resources hosted within Google Cloud Platform utilise additional monitoring sensors as appropriate for each service. Accurate timekeeping for Google production environment is maintained by a series of servers called TimeWarps to ensure a consistent and authoritative view of global time synced across the fleet. A time synchronisation daemon is running on every production server to provide the TrueTime service to all production servers. Redundant time servers in all data centres provide TrueTime service, time synchronisation in the production and edge networks and the Google public NTP. The TrueTime service is further monitored by TrueSnitch, which is an average of several external time sources.

At the core of Google logging is Sawmill, Sawmill is a distributed large-scale system that stores most types of structured, record-orientated data. Upon storage in Sawmill, logs are set to read-only, logs are first frozen so that the meta-data cannot be changed and then set to immutable, indicating the protected read-only mode. As part of the universal encryption effort, logs are encrypted at rest, and logs in transit are also encrypted.

Infrastructure event logs are also managed within Sawmill and stored within Colossus cells, Logs are replicated and stored redundantly in the distributed system. There are three replicas of log data, stored in ten independent locations; further logs are backed up using the Chronicle service, which provides secure storage of read-only files. Security logs are retained for at least 1 year to audit against privileged user access activities, authorised and unauthorised access attempts, and to provide forensic accountability to detect and investigate potential incidents or anomalies.

bernard@numaker.io

5.1.11 Security Intelligence

Google's approach to security intelligence involves leveraging vast amounts of data and advanced analytics to identify and counter threats. Here's how they achieve this:

- **Data Collection:** Google collects data from various sources, including its own products and services, threat intelligence feeds, and public sources. This data encompasses user behavior, network traffic, malware samples, and indicators of compromise.
- **Advanced Analytics:** Google employs sophisticated machine learning algorithms and artificial intelligence to analyze this data, identifying patterns and anomalies that may indicate malicious activity.
- **Threat Detection:** This analysis enables Google to detect a wide range of threats, including malware, phishing attacks, and account hijacking attempts.
- **Proactive Protection:** Google uses the insights gained from its security intelligence to proactively protect its users and systems. For example, they may block malicious websites, flag suspicious emails, or enforce stronger authentication requirements.

- **Information Sharing:** Google shares threat intelligence with other organizations and the security community, helping to improve overall cybersecurity defenses.

Key Components of Google's Security Intelligence

- **VirusTotal:** A service that aggregates data from various antivirus engines and other security tools, providing a comprehensive view of potential threats.
- **Chronicle:** A security analytics platform that leverages Google's infrastructure to provide organizations with advanced threat detection and investigation capabilities.
- **Google Safe Browsing:** A service that protects users from malicious websites by identifying and blocking them in real-time.

Benefits of Google Security Intelligence

- **Enhanced Threat Detection:** Google's vast data and advanced analytics enable them to detect threats that may be missed by traditional security solutions.
- **Proactive Protection:** By identifying threats early, Google can take proactive steps to protect its users and systems before they are compromised.
- **Improved Security Posture:** Google's security intelligence helps organizations to improve their overall security posture by providing them with actionable insights into potential threats.
- **Community Collaboration:** By sharing threat intelligence with the security community, Google helps to raise the bar for cybersecurity defenses across the industry.

bernard@hottaker.io

6 Key Assessment Findings

6.1 Cloud Service Provider Implementation

The objective of this engagement was to assess Google Cloud Platform and Google Workspace , while highlighting the nuances associated with GCVE.

To support the requirements from the Australian Federal Government, Google has identified the need to undergo an independent and comprehensive Cloud Security Assessment, in alignment with the Australian Government's IRAP program. This is required to ensure that all data collected by Google meets the requirements stipulated in the ISM. As such, Google engaged an IRAP assessor to perform the IRAP assessment.

The Sekuro Assessor confirms that based on the findings, observations and interviews conducted, Google Workspace and GCVE is designed in accordance with the March 2024 ISM requirements. The overall architecture, technology in use, policy, standards, and operating procedures are functional and meet requirements of the March 2024 ISM.

6.1.2 Alternate Security Controls

During the assessment, it was found that Google Cloud Platform and Google Workspace were effectively meeting the following control objectives, through an alternate implementation.

Control number(s)	Description of control	Justification for control
ISM-0724	The CISO implements cyber security measurement metrics and key performance indicators for their organisation.	Cyber security metrics and OKRs are implemented via Google Team Leads for their respective departments as per the objectives of the Google Security Program. The Google PSS Team has oversight of the program and defines the key metrics and OKRs. The PSS team is composed of security leaders and these metrics are reported quarterly to the Google Audit and Compliance Committee of the Board (which is composed of executives such as the CISO).
ISM-0718	The CISO reports directly to their organisation's senior executive or Board on cyber security matters.	Cyber security metrics and OKRs are implemented via Google Team Leads for their respective departments as per the objectives of the Google Security Program. The Google PSS Team has oversight of the program and defines the key metrics and OKRs. The PSS team is composed of security leaders and these metrics are reported quarterly to the Google Audit and Compliance Committee of the Board (which is composed of executives such as the CISO).
ISM-0731	The CISO oversees cyber supply chain risk management activities for their organisation.	Due to the size and nature of Google there is a dedicated team to manage supply chain risk which is completed via a robust Vendor Security Assessment. The Vendor Security Audit team reviews the security practices of vendors and the security posture of their products against Google security requirements. The Supply Chain function is responsible for the documentation, review and distribution of the Supply Chain Risk

bernard@bottmaker.ro

Control number(s)	Description of control	Justification for control
		Management Plan. The SCRM plan is required to be reviewed annually by the designated manager or team responsible for supply chain risk management or in case of any event that might trigger an update to the document.
ISM-0732	The CISO receives and manages a dedicated cyber security budget for their organisation.	Google allocates funding to business units at the PA level based on the funding required for each business unit. These budgets are broken down based on prioritisation and assigned to tasks, which includes funding dedicated to cyber security activities in alignment with the Google Security Program. Templates used to determine the budget for a business unit's activities were demonstrated to the Assessor who was able to verify that security/privacy activities are documented within these documents.
ISM-0717	The CISO oversees the management of cyber security personnel within their organisation.	The overall coordination of information security is managed by Royal Hansen, the Vice President of Privacy, Security & Safety. His security responsibilities include overseeing the Security Policy Team, including the formulation and maintenance of security policy and, in coordination with other teams, providing management oversight of the operation of the controls.
ISM-0735	The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.	Google's Security and Privacy Training Team identifies training gaps as information system changes occur. Training materials are updated with new material and deployed during the next training cycle. Google requires that all employees complete annual Privacy & Information Security Training, which includes employee responsibilities for protection of information.
ISM-1636	System owners ensure controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended.	The Security Team performs periodic tests to determine whether controls are properly functioning in the environment and continues to monitor the environment for (new) vulnerabilities and risks to determine whether further controls are necessary. In addition to the activities performed by security engineering, the Certifications & Attestations Team conducts routine sign off and evaluation of control design with control operators. Control revalidation activities in combination with review of open deviations supports management's assessment of control effectiveness.
ISM-1569	A shared responsibility model is created, documented and shared between suppliers and their customers in order to articulate the security responsibilities of each party.	With respect to the customers of Google's own services, a shared responsibility model has been developed and is made publicly available. The model is accessible via the Google Cloud - Cloud Architecture Centre.

bernard@hotmail.com

Control number(s)	Description of control	Justification for control
		Regarding Google's own vendors and suppliers, no shared responsibility models are created and shared. Google incorporates a multi-layered approach within their VSA process which ensures that: • data security and privacy requirements are identified through security and privacy assessments for systems that may be accessed • function of the service provider is identified • appropriate contracts are in place which are defined by the data being accessed and the function to be performed by service providers Google has developed a Master Security Agreement (MSA) template which is used for all supplier/service provider contracting. However, additional contracts may be developed and required to be agreed to prior to any delivery commencing. These additional contracts may come in the forms of ISA, SOW, SDPA, IPA, etc. which define the data used, and associated security responsibilities of each party (Google and the service provider).
ISM-1404	Unprivileged access to systems and applications is disabled after 45 days of inactivity.	For all Google staff who access the corporate and production environment a user requires both the corporate certificate and the production access certificate. After this certificate has been successfully obtained, the user must then retrieve the production access certificate in order to have access to any production environment machines. Both certificates expire after 20 hours which demonstrates automatic disablement of access to the production environment within one day. Additionally, assessors observed that a user is unable to access anything without the certificates in place by viewing the user removing the certificates that were obtained and attempting to access the proprietary service ticket application. The user did not have active certificates, so they were routed to a screen to provide credentials in order to receive active certificates. Google demonstrated that access automatically expires to the environment through the certificate authentication process which mitigates the risk that is posed from not automatically disabling inactive accounts.
ISM-1648	Privileged access to systems and applications is disabled after 45 days of inactivity.	For all Google staff who access the corporate and production environment a user requires both the corporate certificate and the production access certificate. After this certificate has been successfully obtained, the user must then retrieve the production access certificate in order to have access to any production environment machines. Both certificates expire after 20 hours which demonstrates automatic disablement of access to the production environment within one day. Additionally, assessors observed that a user is unable to

bernard@botmail.com

Control number(s)	Description of control	Justification for control
		access anything without the certificates in place by viewing the user removing the certificates that were obtained and attempting to access the proprietary service ticket application. The user did not have active certificates, so they were routed to a screen to provide credentials in order to receive active certificates. Google demonstrated that access automatically expires to the environment through the certificate authentication process which mitigates the risk that is posed from not automatically disabling inactive accounts.
ISM-1716	Access to data repositories is disabled after 45 days of inactivity.	For all Google staff who access the corporate and production environment a user requires both the corporate certificate and the production access certificate. After this certificate has been successfully obtained, the user must then retrieve the production access certificate in order to have access to any production environment machines. Both certificates expire after 20 hours which demonstrates automatic disablement of access to the production environment within one day. Additionally, assessors observed that a user is unable to access anything without the certificates in place by viewing the user removing the certificates that were obtained and attempting to access the proprietary service ticket application. The user did not have active certificates, so they were routed to a screen to provide credentials in order to receive active certificates. Google demonstrated that access automatically expires to the environment through the certificate authentication process which mitigates the risk that is posed from not automatically disabling inactive accounts.
ISM-1647	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.	In order to access the production environment with a Privileged account, the Google Security Team requires a user to authenticate using the Single Sign-On service. Single Sign-On requires a username, password, and second factor authenticator. After this process the user obtains a certificate that allows the user to authenticate to production resources, which use the Machine ACL system as the authorization system of record. This certificate is valid for less than one day. The user session is terminated and needs to be reestablished when this certificate expires, requiring the user to reauthenticate. Users with expired certificates are unable to interact with the production environment, including executing or scheduling new tasks.
ISM-0280	If procuring an evaluated product, a product that has completed a PP-based evaluation, including against all applicable PP modules, is selected in preference to one that has completed an EAL-based evaluation.	Google within the GCI environment produces its own hardware which is subject to robust and stringent requirements, therefore Google does not rely on external vendors for core components. Google designs and procures the necessary hardware based on its own specifications and customises. This ensures

bernard@hotmail.com

Control number(s)	Description of control	Justification for control
		components are tailored to Google's security needs, even without formal PP or EAL evaluations.
ISM-0285	Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.	Google within the GCI environment produces its own hardware which is subject to robust and stringent requirements, therefore Google does not rely on external vendors for core components. Google designs and procures the necessary hardware based on its own specifications and customises. This ensures components are tailored to Google's security needs, even without formal PP or EAL evaluations.
ISM-0289	Evaluated products are installed, configured, administered and operated in an evaluated configuration and in accordance with vendor guidance.	Google within the GCI environment produces its own hardware which is subject to robust and stringent requirements, therefore Google does not rely on external vendors for core components. Google designs and procures the necessary hardware based on its own specifications and customises. This ensures components are tailored to Google's security needs, even without formal PP or EAL evaluations. Therefore the above hardware is installed, configured, administered and operated in a manner that is equivalent.
ISM-1361	Security Construction and Equipment Committee-approved equipment or ASIO-approved equipment is used when destroying media.	During the onsite walkthrough of Sydney Datacenters the assessor noted the equipment used for destruction, the shredders and punch devices meet the data destruction requirements outlined by the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a recognized U.S. government-wide program for assessing and approving cloud service offerings for security. Meeting these requirements ensures the effectiveness of Google's data destruction equipment in securely erasing information from various media types.
ISM-1745	Early Launch Antimalware, Secure Boot, Trusted Boot and Measured Boot functionality is enabled.	Google takes an alternate approach to managing features of this control through the use of Container Threat Detection (CTD), This is a built-in service of Security Command Center that continuously monitors the state of Container-Optimized OS node images. The service evaluates all changes and remote access attempts to detect runtime attacks in near-real time. Container Threat Detection includes several detection capabilities, including suspicious binaries and libraries, and uses natural language processing (NLP) to detect malicious Bash and Python code.

bernard@bitmaker.io

Control number(s)	Description of control	Justification for control
ISM-1592	Unprivileged users do not have the ability to install unapproved software.	Google configures machines to provide only essential capabilities. Google enforces least functionality on machines by minimizing functionality to the baseline configuration that is pushed out through its proprietary build tool. The baseline configuration restricts functionality to only essential capabilities. Google utilizes Bit9 which is a binary control agent that is capable of blocking unrecognized or unapproved binaries from execution on Servers and Workstations. When a server is in the default Lockdown mode, unknown binaries are blocked unless they are explicitly allowed. Managing the allowlist is facilitated by Upvote. Social allowlisting works the same on servers as it does on workstations. This is the standard allowlisting method, and is sufficient for most cases. Users whilst they have the ability to install software upvote require only 2 votes to locally allow a binary. Allowed binaries can run on machines that you have logged into.
ISM-1795	Credentials for break glass accounts, local administrator accounts and service accounts are a minimum of 30 characters.	The assessor reviewed the evidence provided throughout workshops with Google technical SME's, it was noted that not all accounts within the categories listed within this control meet the minimum 30 character minimum, However strong mitigating controls are in place to ensure security, This includes but not limited to: *Multi-factor authentication (MFA): All privileged accounts require MFA for access to the production environment. * Device and user certificate authentication * Regular password rotation and complexity * Stringent monitoring
ISM-1387	Administrative activities are conducted through jump servers.	The Google Security Team only authorizes remote access through a single path to access production resources that requires use of the Single Sign-On service using a production based workstations managed by Google. Single Sign-On requires a username, password, and second factor authenticator. After this process the user obtains a certificate that allows the user to authenticate to production resources. In order to connect to a remote resource using this method, the user is required to be in an authorized Machine ACL group as well as be using an authorized device.
ISM-1905	Online services that are no longer supported by vendors are removed.	There are times when unsupported components may need to remain on the network to manage legacy applications and systems. When this

bernard@botmail.com

Control number(s)	Description of control	Justification for control
		occurs, Production Support will perform additional activities on legacies systems to ensure the system is monitored. This may include: 1. Privacy incident handling / remediation ensures high quality and timeliness of one-off issue resolution, along with filing and actioning of formal Incident Report procedures as needed (i.e. where no product owner is available to do so). 2. Mitigation / prevention includes driving needed repairs to address incorrect legacy system behavior where feasible, as well as managing risks during end-of-life for deprecated platform components. Learnings from current incident experience are leveraged to provide requirements, technical design, and transition plans for next generation privacy solutions. 3. Transition / deprecation activities prepare legacy and end-of-life systems for turndown, including cleanup and safe migration of current data. 4. Support process definition ensures frontline agents have all needed tools and guidance to handle user information securely and accurately, conforming to Google Cloud best practices for user data privacy and keeping pace with emerging regulatory/certification requirements. 5. Consultation across the Cloud Systems organization (and the entire Google Cloud business) ensures questions regarding complaint handling of user data receive SME attention, whether helping PS frontline agents to resolve specific support cases or reviewing privacy content in next generation product designs.
ISM-0304	Applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	There are times when unsupported components may need to remain on the network to manage legacy applications and systems. When this occurs, Production Support will perform additional activities on legacies systems to ensure the system is monitored. This may include: 1. Privacy incident handling / remediation ensures high quality and timeliness of one-off issue resolution, along with filing and actioning of formal Incident Report procedures as needed (i.e. where no product owner is available to do so). 2. Mitigation / prevention includes driving needed repairs to address incorrect legacy system behavior where feasible, as well as managing risks during end-of-life for deprecated platform components. Learnings from current incident experience are leveraged to provide requirements, technical design, and transition plans for next generation privacy solutions.

bernard@botmaker.com

Control number(s)	Description of control	Justification for control
		3. Transition / deprecation activities prepare legacy and end-of-life systems for turndown, including cleanup and safe migration of current data. 4. Support process definition ensures frontline agents have all needed tools and guidance to handle user information securely and accurately, conforming to Google Cloud best practices for user data privacy and keeping pace with emerging regulatory/certification requirements. 5. Consultation across the Cloud Systems organization (and the entire Google Cloud business) ensures questions regarding complaint handling of user data receive SME attention, whether helping PS frontline agents to resolve specific support cases or reviewing privacy content in next generation product designs.
ISM-1501	Operating systems that are no longer supported by vendors are replaced.	There are times when unsupported components may need to remain on the network to manage legacy applications and systems. When this occurs, Production Support will perform additional activities on legacies systems to ensure the system is monitored. This may include: 1. Privacy incident handling / remediation ensures high quality and timeliness of one-off issue resolution, along with filing and actioning of formal Incident Report procedures as needed (i.e. where no product owner is available to do so). 2. Mitigation / prevention includes driving needed repairs to address incorrect legacy system behavior where feasible, as well as managing risks during end-of-life for deprecated platform components. Learnings from current incident experience are leveraged to provide requirements, technical design, and transition plans for next generation privacy solutions. 3. Transition / deprecation activities prepare legacy and end-of-life systems for turndown, including cleanup and safe migration of current data. 4. Support process definition ensures frontline agents have all needed tools and guidance to handle user information securely and accurately, conforming to Google Cloud best practices for user data privacy and keeping pace with emerging regulatory/certification requirements. 5. Consultation across the Cloud Systems organization (and the entire Google Cloud business) ensures questions regarding

bernard@botmail.com

Control number(s)	Description of control	Justification for control
		complaint handling of user data receive SME attention, whether helping PS frontline agents to resolve specific support cases or reviewing privacy content in next generation product designs.
ISM-1753	Network devices and other ICT equipment that are no longer supported by vendors are replaced.	There are times when unsupported components may need to remain on the network to manage legacy applications and systems. When this occurs, Production Support will perform additional activities on legacies systems to ensure the system is monitored. This may include: 1. Privacy incident handling / remediation ensures high quality and timeliness of one-off issue resolution, along with filing and actioning of formal Incident Report procedures as needed (i.e. where no product owner is available to do so). 2. Mitigation / prevention includes driving needed repairs to address incorrect legacy system behavior where feasible, as well as managing risks during end-of-life for deprecated platform components. Learnings from current incident experience are leveraged to provide requirements, technical design, and transition plans for next generation privacy solutions. 3. Transition / deprecation activities prepare legacy and end-of-life systems for turndown, including cleanup and safe migration of current data. 4. Support process definition ensures frontline agents have all needed tools and guidance to handle user information securely and accurately, conforming to Google Cloud best practices for user data privacy and keeping pace with emerging regulatory/certification requirements. 5. Consultation across the Cloud Systems organization (and the entire Google Cloud business) ensures questions regarding complaint handling of user data receive SME attention, whether helping PS frontline agents to resolve specific support cases or reviewing privacy content in next generation product designs.
ISM-1801	Network devices are restarted on at least a monthly basis.	Google's production network, built on virtualization, makes traditional hardware restarts impractical and potentially disruptive. The network is designed with redundancy and failover systems to maintain critical functions, even during individual device or update issues. Google employs rolling deployments for software updates to minimize disruption and ensure service continuity.
ISM-1774	Gateways are managed via a secure path isolated from all connected networks.	To access Prod, Google verifies the user's identity utilizing the Single Sign-On service,

bernard@botmail.ro

Control number(s)	Description of control	Justification for control
		which prompts for the username, password, 2FA, and long-lived machine certificate to obtain an SSH, LOAS, or an SSO token. All these output credentials are valid for less than a day (See IA-2), and are bound to the long-lived machine certificate. These credentials allow a user to authenticate to machine resources, which use the Machine ACL system as the authorization system of record and networking devices using the Network AAA service as the authorization system of record. Thus, Machine ACL system and the Network AAA service provide the account management functions in Prod as it pertains to the controls requirements in the AC family. Google does not permit external remote connections into Prod. The only path to Prod is through the Single Sign-On service and using workstations/laptops managed by Google, this meets the intent of the control via an alternate method.
ISM-1876	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1690	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and

bernard@botmail.com

Control number(s)	Description of control	Justification for control
		provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1691	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1692	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in

bernard@botmak...

Control number(s)	Description of control	Justification for control
		place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1901	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1693	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability

bernat@botmail.cl

Control number(s)	Description of control	Justification for control
		(KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement.
ISM-1877	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1694	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which

bernard@botmail.com

Control number(s)	Description of control	Justification for control
		meets the intent or removing or lowering the risk of the vulnerability.
ISM-1695	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1696	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which

bernard@botmail.com

Control number(s)	Description of control	Justification for control
		meets the intent or removing or lowering the risk of the vulnerability.
ISM-1902	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1878	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of ICT equipment other than workstations, servers and network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which

bernard@botmail

Control number(s)	Description of control	Justification for control
		meets the intent or removing or lowering the risk of the vulnerability.
ISM-1751	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of ICT equipment other than workstations, servers and network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1879	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which

bernard@botmail

Control number(s)	Description of control	Justification for control
		meets the intent or removing or lowering the risk of the vulnerability.
ISM-1697	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1903	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which

bernard@botmail

Control number(s)	Description of control	Justification for control
		meets the intent or removing or lowering the risk of the vulnerability.
ISM-1904	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	The Assessor reviewed the FedRAMP SSP and noted that Google security team members assist to mitigate legitimate high-risk vulnerabilities within 30 days, moderate-risk vulnerabilities within 90 days, low-risk vulnerabilities within 180 days. In the event that Google is unable to mitigate a high, moderate, or low-risk vulnerability within these FedRAMP-required remediation timeliness, Google will report these items to all FedRAMP stakeholders as an overdue POA&M item and provide mitigation updates through monthly POA&M submissions. Google has a process in place to verify when vulnerabilities are listed among the CISA Known Exploited Vulnerability (KEV) Catalog and to modify the SLA when the KEV remediation date supersedes the FedRAMP parameter requirement. While Google's approach to patching critical vulnerabilities in online services is well-defined and aligns with FedRamp requirements it deviates from the specific timeframe stipulated by this control, Google SME's acknowledged the use of alternative measures to lower or mitigate the risk such as configuration changes or network restrictions to the environment which meets the intent or removing or lowering the risk of the vulnerability.
ISM-1403	Accounts, except for break glass accounts, are locked out after a maximum of five failed logon attempts.	User accounts are locked out if more than 30 failed login attempts using only password (e.g., login to machine) occur within a 3 hour period. There is no lockout when using the cryptographic token (e.g., when authenticating to Single Sign-on system) because the signatures are inherently brute-force proof. The main focus of this control is to prevent brute force attacks against accounts authenticated using usernames and passwords. Google has implemented stronger authentication mechanisms including username, passwords, and the required use of a phishing resistant second factor authenticator throughout the Google infrastructure. The second factor authenticator provides an additional layer of protection in case the user's regular password is compromised. An adversary would need to compromise both the regular password and physically the second factor authenticator as this hardware authenticator requires a physical touch to close an electrical circuit that can not be closed remotely.
ISM-0294	ICT equipment, with the exception of high assurance ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.	It was reviewed during the onsite visit by the assessor to the facilities in scope that equipment is not labelled to identify its sensitivity or classification.

bernard@botmail.com

Control number(s)	Description of control	Justification for control
ISM-0332	Media, with the exception of internally mounted fixed media within ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.	The assessor reviewed samples of media and there were no labels to identify its sensitivity or classification.

Table 7: GCP and Workspace Alternate Controls

The Following Alternate Control was identified that is applicable only to Google Cloud VMware Engine:

Control number(s)	Description of control	Justification for control
ISM-1789	Sufficient spares of critical ICT equipment are sourced and kept in reserve.	For the GCVE Environment spares are not kept onsite, Instead contractual agreements are in place for warranty SLA's to ensure replacment parts are sourced and delivered in a suitable timeframe.

Table 8: GCVE Alternate Control

6.1.3 Security Controls Not Implemented due to Business Decision

Due to operational requirements, Google has decided not to implement the following ISM controls. NIST SP 800-30 (risk management)[14] is referenced as a resource for Google to understand the residual risk and the assessment of these not implemented controls.

Control number(s)	Description of control	Operational requirements rationale and mitigating factors
N/A	N/A	N/A

Table 9: Not Implemented Controls

6.1.4 Ineffective Security Controls

During the assessment, it was found that Google was not effectively meeting the following control objectives. Where appropriate, the Assessor has listed any recommended remediation, or any remediation that is currently planned by Google.

Control number(s)	Description of control	Justification
ISM-1737	A managed service register contains the following for each managed service: • managed service provider's name • managed service's name • purpose for using the managed service • sensitivity or classification of data involved	The subprocessor lists are made publicly available and record the following information: • subprocessor's name • activities which the subprocessor performs for Google

[14] NIST SP 800-30 Resource Page:
https://www.nist.gov/privacy-framework/nist-sp-800-30

bernardo@hotmail.com

Control number(s)	Description of control	Justification
	• due date for the next security assessment of the managed service • contractual arrangements for the managed service • point of contact for users of the managed service • 24/7 contact details for the managed service provider.	• relevant Google services that use this subprocessor • countries where the processing is performed • registered address of the subprocessor • country where the subprocessor is registered • company number for the subprocessor • parent company of subprocessors. The information captured within these registers are not in alignment with the ISM requirements for service registers. Information such as contact details, classification of data handled, due dates for next security assessments are captured across Buying Hub portals/categories and within contractual agreements, however, this does not follow the centralised approach as per the intent of this ISM control.
ISM-1793	Managed service providers and their managed services undergo a security assessment by an IRAP assessor at least every 24 months.	Entities listed within Google's public facing subprocessor list are not all IRAP assessed, nor is the completion of an IRAP assessment observed to be a requirement/factor within Google's Vendor Security Assessment (VSA) process.
ISM-1638	An outsourced cloud service register contains the following for each outsourced cloud service: • cloud service provider's name • cloud service's name • purpose for using the cloud service • sensitivity or classification of data involved • due date for the next security assessment of the cloud service • contractual arrangements for the cloud service • point of contact for users of the cloud service • 24/7 contact details for the cloud service provider.	The subprocessor lists are made publicly available and record the following information: • subprocessor's name • activities which the subprocessor performs for Google • relevant Google services that use this subprocessor • countries where the processing is performed • registered address of the subprocessor • country where the subprocessor is registered • company number for the subprocessor • parent company of sub processor. The information captured within these registers are not in alignment with the ISM requirements for service registers. Information such as contact details, classification of data handled, due dates for next security assessments are captured across Buying Hub portals/categories and within contractual agreements, however, this does not follow the centralised approach as per the intent of this ISM control.

bernard@hotmail.com

Control number(s)	Description of control	Justification
ISM-1570	Outsourced cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months.	Entities listed within Google's public facing subprocessor list are not all IRAP assessed, nor is the completion of an IRAP assessment observed to be a requirement/factor within Google's Vendor Security Assessment (VSA) process.
ISM-1571	The right to verify compliance with security requirements is documented in contractual arrangements with service providers.	The assessor reviewed a sample of contracts including MSA,SDPA via an online workshop, It was identified that some contracts did not contain the right to verify.
ISM-1163	Systems have a continuous monitoring plan that includes: • conducting vulnerability scans for systems at least fortnightly • conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter • analysing identified vulnerabilities to determine their potential impact • implementing mitigations based on risk, effectiveness and cost.	Continuous monitoring plans are defined and captured within SSP appendices (GCP, GCI, Workspace) and were made available to the Assessor for review. These plans define Google's continuous scanning processes which underpin the Plan of Action and Milestones (POA&M) process for Google Services and Workspace respectively, and are aligned to FedRAMP requirements. The continuous monitoring plans requires: • conducting vulnerability scans for systems monthly • annual penetration testing activities • analysing identified vulnerabilities to determine their potential impact through Google Bug Review • update POA&M registers with the latest vulnerabilities for tracking and remediation Further, the Continuous Monitoring (ConMon) Program for Google Services includes Google Workspace. The same processes/controls that live on Google Common Infrastructure (GCI) that are part of the Google Services authorization, from the scanning process to vuln tracking and report generation, are leveraged by Google Workspace. Each month GCI is providing a ConMon service to Google Workspace that includes the delivery of ConMon reports, which are in turn used to meet Google Workspace's ConMon reporting requirements.
ISM-1724	Magnetic hard disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or degausser.	It was reviewed by the assessor that magnetic hard drives are destroyed via a SEM manufactured automated hard drive crusher prior to being released to scrap metal. If the magnetic hard disk is functional before it is sent for repair and prior to removal, an automated system triggers an online disk erase process to sanitize the disk before releasing the repair tasks to technicians, However if the disk is not functional this process cannot be carried out.

bernardobotmanno@gmail.com

Control number(s)	Description of control	Justification
ISM-0361	Magnetic media is destroyed using a degausser with a suitable magnetic field strength and magnetic orientation.	The assessor reviewed the destruction process for magnetic media whilst on site during the Datacenter walkthrough and noted that a SEM punch tool is used to damage the hard drives.
ISM-1874	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.	Whilst Multifactor authentication is the responsibility of the consumer Google Workspace offers a wide range of options for consumers to utilize to ensure a phishing resistant approach is adopted, This includes hardware-based solutions such as FIDO2 keys and mobile device authentication. However non-phishing resistant options are also available for use such as TOTP.
ISM-1698	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool. The 3PAO also regularly audits Google's internal scan tools to ensure that they are working correctly.
ISM-1699	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool. The 3PAO also regularly audits Google's internal scan tools to ensure that they are working correctly.
ISM-1700	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool. The 3PAO also regularly audits Google's internal

bernard@bot

Control number(s)	Description of control	Justification
		scan tools to ensure that they are working correctly.
ISM-1701	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.	The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool. The 3PAO also regularly audits Google's internal scan tools to ensure that they are working correctly.
ISM-1702	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.	The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool. The 3PAO also regularly audits Google's internal scan tools to ensure that they are working correctly.
ISM-1752	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of ICT equipment other than workstations, servers and network devices.	The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool. The 3PAO also regularly audits Google's internal scan tools to ensure that they are working correctly.
ISM-1703	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.	The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool.

bernard@otmake.com

Control number(s)	Description of control	Justification
		The 3PAO also regularly audits Google's internal scan tools to ensure that they are working correctly.
ISM-1900	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.	The Google Security Team performs monthly infrastructure and web application scans, and proprietary database checks as part of Google's continuous monitoring vulnerability management process. Monthly scans consist of internal scans of the GCI using Google's proprietary vulnerability scanning tools and are monitored continuously. External web applications are scanned monthly by a 3PAO using a COTS vulnerability scan tool. The 3PAO also regularly audits Google's internal scan tools to ensure that they are working correctly.

Table 10: GCP and Workspace Ineffective Controls

6.1.5 No Visibility Security Controls

During the assessment, the Assessor was unable to obtain adequate visibility of the implementation of the following controls.

Control number(s)	Description of control
ISM-0140	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
ISM-1783	Public IP addresses controlled by, or used by, an organisation are signed by valid ROA records.

Table 11: GCP and Workspace No Visibility Controls

bernard@lotnak.com

APPENDIX A Cloud Controls Matrix

To open the CCM document in Microsoft Excel:

- Use the latest version of Adobe Acrobat Reader to open this report.
- Click the paperclip icon · in the Navigation pane to the left of this document.
- Double-click the excel file.
- If there is no paper clip showing, then click on View Show/Hide Navigation Panes Attachments. In some versions, to get the paper clip, click on View Navigation Panes Attachments. This will also open the attachments pane in Adobe Reader.

bernard@botmaker.io

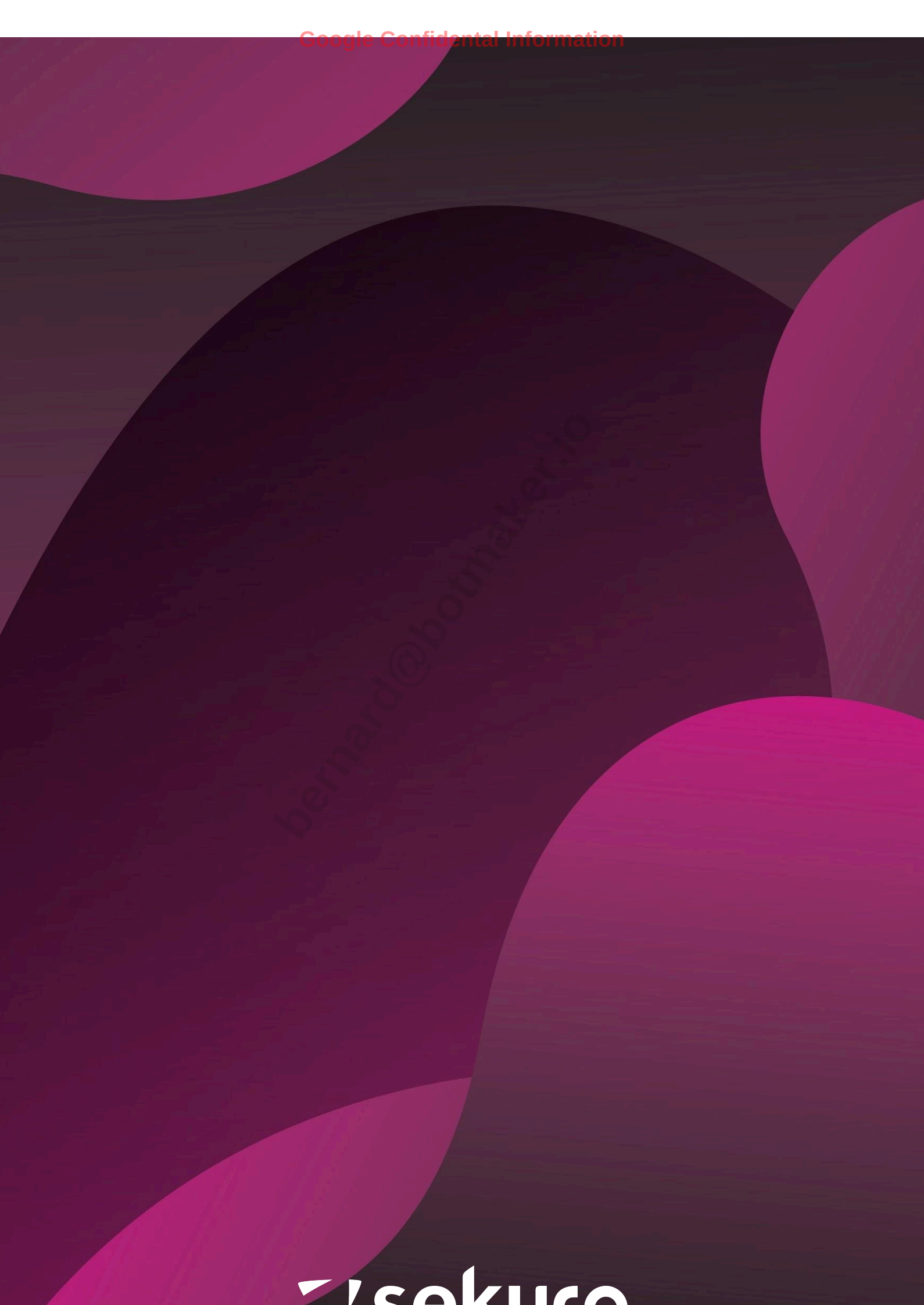
APPENDIX B Addendums

Consumers of Google's services should check with Google for any addendums to this report. Google aims to independently verify addendum contents by an IRAP Assessor through their compliance program. These addendums are provided by Google to maintain the accuracy and validity of their reports between independent assessments. Cloud Consumers need to consider any lack of independent verification when reviewing the addendums.

bernard@botmaker.io

Google Confidental Information

bernard@botmaker.io



Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Payment Card Industry

Data Security Standard

bernard@botmaker.io

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

bernard@botmaker.io

Entity Name: Google LLC

Date of Report as noted in the Report on Compliance: 12/09/2024

Date Assessment Ended: 11/30/2024

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)	
Company name:	Google LLC
DBA (doing business as):	Google Cloud Platform (GCP)
Company mailing address:	1600 Amphitheatre Pkwy Mountain View, CA 94043
Company main website:	https://cloud.google.com
Company contact name:	Jeanette Manfra
Company contact title:	Senior Director, Global Risk and Compliance (Cloud CISO)
Contact phone number:	650-253-0000
Contact e-mail address:	gcp-pci@google.com

Part 1b. Assessor (ROC Section 1.1)	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Joe Nangle
Qualified Security Assessor	
Company name:	Coalfire Systems, Inc.
Company mailing address:	8480 E Orchard Rd., Suite 5800 Greenwood Village, CO 80111
Company website:	https://www.coalfire.com
Lead Assessor name:	David Miller
Assessor phone number:	877-224-8077
Assessor e-mail address:	CoalfireSubmission@coalfire.com

bernard@notmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Assessor certificate number:	QSA # 206-014

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	The following GCP services were included in this assessment: 1. Access Approval 2. Access Context Manager 3. Access Transparency 4. Advanced API Security 5. Agent Assist 6. AI Platform Deep Learning Container 7. AI Platform Training and Prediction 8. AlloyDB 9. Anti-Money Laundering AI 10. API Gateway 11. Apigee 12. App Engine 13. Application Integration 14. AppSheet (GCP) 15. Artifact Analysis 16. Artifact Registry 17. Assured Workloads 18. AutoML Natural Language 19. AutoML Tables 20. AutoML Translation 21. AutoML Video 22. AutoML Vision 23. Backup and DR Service 24. Backup for GKE 25. Bare Metal HSM 26. Bare Metal Rack HSM 27. Batch 28. BigQuery 29. BigQuery Data Transfer Service 30. Binary Authorization 31. CCAI Platform 32. Certificate Authority Service 33. Certificate Manager 34. Chrome Enterprise Premium (formerly BeyondCorp Enterprise) 35. Cloud Asset Inventory 36. Cloud Bigtable 37. Cloud Billing 38. Cloud Build 39. Cloud CDN 40. Cloud Composer 41. Cloud Console 42. Cloud Console App 43. Cloud Data Fusion 44. Cloud Deployment Manager 45. Cloud DNS 46. Cloud Endpoints 47. Cloud External Key Manager (Cloud EKM) 48. Cloud Filestore

bernard@notarize.com

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

	49. Cloud Functions 50. Cloud Functions for Firebase 51. Cloud Healthcare 52. Cloud HSM 53. Cloud Identity 54. Cloud IDS (Cloud Intrusion Detection System) 55. Cloud Interconnect 56. Cloud Key Management Service 57. Cloud Life Sciences 58. Cloud Load Balancing 59. Cloud Logging 60. Cloud Monitoring 61. Cloud NAT (network address translation) 62. Cloud Natural Language API 63. Cloud NGFW (formerly Cloud Firewall) 64. Cloud Profiler 65. Cloud Router 66. Cloud Run 67. Cloud Scheduler 68. Cloud Service Mesh 69. Cloud Shell 70. Cloud Source Repositories 71. Cloud Spanner 72. Cloud Speaker ID 73. Cloud SQL 74. Cloud Storage 75. Cloud Storage for Firebase 76. Cloud Tasks 77. Cloud Trace 78. Cloud Translation 79. Cloud Vision 80. Cloud VPN 81. Cloud Workstations 82. Compute Engine 83. Connect 84. Contact Center AI (CCAI) 85. Contact Center AI Insights 86. Container Registry 87. Data Catalog 88. Database Migration Service 89. Dataflow 90. Dataform 91. Dataplex 92. Dataproc 93. Dataproc Metastore 94. Datastore 95. Datastream 96. Dialogflow 97. Document AI 98. Document AI Warehouse 99. Eventarc 100. Firebase App Check 101. Firebase Authentication 102. Firestore 103. Gemini for Google Cloud 104. Generative AI on Vertex AI 105. GKE Enterprise Config Management 106. GKE Identity Service

bernard@brokerio

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

	107. Google Cloud Armor 108. Google Cloud Deploy 109. Google Cloud Identity-Aware Proxy 110. Google Cloud Marketplace 111. Google Cloud SDK 112. Google Cloud VMware Engine (GCVE) 113. Google Kubernetes Engine 114. Google Security Operations (SIEM) 115. Google Security Operations (SOAR) 116. GTI for Google Security Operations 117. Healthcare Data Engine 118. Hub 119. Identity & Access Management (IAM) 120. Identity Platform 121. Infrastructure Manager 122. Integration Connectors 123. Key Access Justifications (KAJ) 124. Knative Serving 125. Looker (Google Cloud core) 126. Looker Studio 127. Managed Service for Microsoft Active Directory (AD) 128. Media CDN 129. Memorystore 130. Migrate to Virtual Machines 131. Migration Center 132. Network Connectivity Center 133. Network Intelligence Center 134. Network Service Tiers 135. Persistent Disk 136. Personalized Service Health 137. Privileged Access Manager 138. Pub/Sub 139. Ray on Vertex 140. reCAPTCHA Enterprise 141. Recommender 142. Resource Manager API 143. Risk Manager 144. SecLM 145. Secret Manager 146. Secure Source Manager 147. Secure Web Proxy (Cloud SWP) 148. Security Command Center 149. Sensitive Data Protection (including Cloud Data Loss Prevention) 150. Service Directory 151. Service Infrastructure 152. Service Mesh 153. Speech-to-Text 154. Storage Transfer Service 155. Talent Solution 156. Text-to-Speech 157. Traffic Director 158. Transfer Appliance 159. Vertex AI Codey 160. Vertex AI Colab Enterprise 161. Vertex AI Conversation 162. Vertex AI Data Labeling 163. Vertex AI Platform 164. Vertex AI Search

bernard@workaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

	165. Vertex AI Workbench Instances 166. Video Intelligence API 167. Virtual Private Cloud 168. VPC Service Controls 169. Web Risk API 170. Workflows 171. Workload Manager

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☒ Applications / software	☒ Systems security services	☐ POI / card present
☒ Hardware	☐ IT support	☐ Internet / e-commerce
☒ Infrastructure / Network	☒ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☒ Storage	☒ Other services (specify):	☐ Other processing (specify):
☒ Web-hosting services	Software as a Service (SaaS)	
☒ Security services	Infrastructure as a Service (IaaS)	
☐ 3-D Secure Hosting Provider	Platform as a Service (PaaS)	
☒ Multi-Tenant Service Provider	Function as a Service (FaaS)	
☐ Other Hosting (specify):	Containers as a Service (CaaS)	
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		

☐ Others (specify): Not Applicable

Provide a brief explanation why any checked services were not included in the Assessment:	Not Applicable

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	Google Cloud Platform (GCP) does not store, process, or transmit account data for its own business. GCP customers are responsible for the security of the account data they store, process, or transmit.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Google Cloud Platform (GCP) customers build their CDEs using Google Cloud services. The security and compliance of these services directly affects the security and compliance of the customer's services.
Describe system components that could impact the security of account data.	GCP does not directly store, process, or transmit account data for its own business. However, Google Cloud Platform, GCP products may be used by

bernard@hotmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

	customers to host or support their cardholder data environment (CDE). Therefore, the GCP environment was assessed with the assumption all customer data was account data, but GCP customers are responsible for their own PCI DSS compliance. System components within the CDE that could impact the security of account data: • Firewalls, routers, and switches • Servers • Storage • Encryption and Key Management Support Systems • Administrative Workstations/Laptops • Multi-factor authentication • Access Authorization • Change Management • File Integrity Monitoring • Intrusion Detection Systems • Logging and Alerting • Internal Vulnerability Scanning • External ASV Scanning • Penetration Testing

bernard@botmakers.co

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	GCP offers its customers IaaS, PaaS, SaaS, FaaS and CaaS solutions, which may be used by customers to host their cardholder data environment (CDE) to store, process, or transmit account data. The critical system components within the CDE that were assessed include: • Firewalls, routers, and switches • Servers • Storage • Encryption and Key Management Support Systems • Administrative Workstations/Laptops • Multi-factor authentication • Access Authorization • Change Management • File Integrity Monitoring • Intrusion Detection Systems • Logging and Alerting • Internal Vulnerability Scanning • External ASV Scanning • Penetration Testing
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Google Data Centers	137	North America • Arcola, VA, United States of America • Ashburn (1), VA, United States of America • Ashburn (2), VA, United States of America • Ashburn (3), VA, United States of America

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		• Ashburn (IAD39), VA, United States of America • Atlanta (1), GA, United States of America • Atlanta (2), GA, United States of America • Chandler, AZ, United States of America • Clarksville, TN, United States of America • Columbus (1), OH, United States of America • Columbus (2), OH, United States of America • Council Bluffs (1), IA, United States of America • Council Bluffs (2), IA, United States of America • Council Bluffs (CBF65), IA, United States of America • Gainesville, VA, United States of America • Guanajuato, Mexico • Henderson, NV, United States of America • Hillsboro (HIO03), OR, United States of America • Lancaster, OH, United States of America • Las Vegas, NV, United States of America • Leesburg, VA, United States of America • Lenoir, NC, United States of America • Los Angeles (1), CA, United States of America • Los Angeles (2), CA, United States of America • Los Angeles (3), CA, United States of America • Markham, ON, Canada • Midlothian, TX, United States of America • Midlothian (DFW36), TX, United States of America • Moncks Corner, SC, United States of America • Montreal (1), QC, Canada • Montreal (2), QC, Canada • New Albany, OH, United States of America

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		• Omaha, NE, United States of America • Papillion, NE, United States of America • Phoenix (1), AZ, United States of America • Pryor Creek, OK, United States of America • Reno, NV, United States of America • Salt Lake City (1), UT, United States of America • Salt Lake City (2), UT, United States of America • Salt Lake City (3), UT, United States of America • The Dalles (1), OR, United States of America • The Dalles (2), OR, United States of America • Toronto (2), ON, Canada • Toronto, ON, Canada • Widows Creek, AL, United States of America South America • Osasco, Brazil • Quilicura (1), Santiago, Chile • Quilicura (2), Santiago, Chile • Quilicura (3), Santiago, Chile • San Bernardo, Santiago, Chile • Santana de Parnaíba, Brazil • Vinhedo, Brazil Asia Pacific • Changhua, Taiwan • Delhi (1), India • Delhi (2), India • Delhi (3), India • Hong Kong (1), Hong Kong • Hong Kong (2), Hong Kong • Hong Kong (3), Hong Kong • Inzai, Chiba, Japan • Jakarta (1), Indonesia • Jakarta (2), Indonesia • Jakarta (3), Indonesia • Koto-ku (1), Tokyo, Japan • Koto-ku (2), Tokyo, Japan • Koto-ku (3), Tokyo, Japan • Lok Yang Way, Singapore • Loyang, Singapore • Melbourne (1), Australia • Melbourne (2), Australia • Melbourne (3), Australia

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		• Mumbai (1), India • Mumbai (2), India • Mumbai (3), India • Mumbai (4), India • Osaka (1), Japan • Osaka (2), Japan • Seoul (1), South Korea • Seoul (2), South Korea • Seoul (3), South Korea • Sydney (1), NSW, Australia • Sydney (2), NSW, Australia • Sydney (3), NSW, Australia • Sydney (4), NSW, Australia • Wenya, Singapore EMEA • Berlin (1), Germany • Berlin (2), Germany • Berlin (3), Germany • Dalarna, Sweden • Dammam, Saudi Arabia • Doha (1), Qatar • Doha (2), Qatar • Doha (3), Qatar • Dublin, Ireland • Eemshaven, Groningen, the Netherlands • Eemshaven (GRQ23), Groningen, the Netherlands • Frankfurt (1), Hesse, Germany • Frankfurt (2), Hesse, Germany • Frankfurt (4), Hesse, Germany • Frankfurt (5), Hesse, Germany • Frankfurt (6), Hesse, Germany • Frankfurt (7), Hesse, Germany • Frankfurt (8), Hesse, Germany • Frankfurt (FRA56), Hesse, Germany • Fredericia, Denmark • Ghlin, Hainaut, Belgium • Hamina, Finland • London (1), United Kingdom • London (3), United Kingdom • London (4), United Kingdom • London (5), United Kingdom • London (6), United Kingdom • Madrid (1), Spain • Madrid (2), Spain • Madrid (3), Spain • Middenmeer, Noord-Holland, the Netherlands • Milan (1), Italy • Milan (2), Italy

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		• Milan (3), Italy • Paris (1), France • Paris (2), France • Paris (3), France • Tel Aviv (1), Israel • Tel Aviv (2), Israel • Tel Aviv (3), Israel • Turin (1), Italy • Turin (2), Italy • Turin (3), Italy • Warsaw (1), Poland • Warsaw (2), Poland • Warsaw (3), Poland • Zurich (1), Switzerland • Zurich (2), Switzerland • Zurich (3), Switzerland Africa • Johannesburg (1), South Africa • Johannesburg (2), South Africa • Johannesburg (3), South Africa
TPSP Hosted Data Centers	28	Ascenty • Sao Paulo, Brazil Cologix • Quebec, Canada CyrusOne • Council Bluffs, Iowa, USA • Sterling, Virginia, USA Databank • Los Angeles, California, USA (2) DigitalRealty • Frankfurt, Germany (2) • Sydney, Australia Equinix • Ashburn, Virgina, USA (2) • Dallas, Texas, USA • Frankfurt, Germany (2) • London, United Kingdom • Ontario, Canada • Tai Seng Drive, Singapore • Tokyo, Japan Global Data Centers / Edgeconnex • Tel Aviv, Israel GreenDC • Zurich, Switzerland GTD • Santiago, Chile

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		Macquarie • Sydney, Australia NetMagic • Mumbai, India Noovle • Milan, Italy QTS • Eemshaven, Netherlands SDS Data • Tel Aviv, Israel Sify • New Delhi, India Virtus • London, United Kingdom
Corporate Offices (not in scope for Requirement 9.x)	138	North America • Addison, TX, United States of America • Alexandria, VA, United States of America • Ann Arbor, MI, United States of America • Atlanta, GA, United States of America • Austin, TX, United States of America • Bellevue, WA, United States of America • Boston, MA, United States of America • Bothell, WA, United States of America • Boulder, CO, United States of America • Calgary, AB, Canada • Cambridge, MA, United States of America • Charlotte, NC, United States of America • Chicago, IL, United States of America • Detroit, MI, United States of America • Durham, NC, United States of America • Fremont, CA, United States of America • Goleta, CA, United States of America

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		• Houston, TX, United States of America • Irvine, CA, United States of America • Kirkland, WA, United States of America • Kitchener, ON, Canada • Los Angeles, CA, United States of America • Madison, WI, United States of America • Mexico City, Mexico • Miami, FL, United States of America • Montreal, QC, Canada • Mountain View, CA, United States of America • Mountain View, CA, United States of America • Nashville, TN, United States of America • New York, NY, United States of America • Ottawa, ON, Canada • Palo Alto, CA, United States of America • Pittsburgh, PA, United States of America • Playa Vista, CA, United States of America • Portland, OR, United States of America • Poughkeepsie, NY, United States of America • Princeton, NJ, United States of America • Redmond, WA, United States of America • Redwood City, CA, United States of America • Reston, VA, United States of America • Salt Lake City, UT, United States of America • San Bruno, CA, United States of America • San Diego, CA, United States of America • San Francisco, CA, United States of America • San Jose, CA, United States of America • Santa Cruz, CA, United States of America

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		• Seattle, WA, United States of America • South San Francisco, CA, United States of America • Southaven, MS, United States of America • Sunnyvale, CA, United States of America • Thornton, CO, United States of America • Toronto, ON, Canada • Vancouver, BC, Canada • Washington D.C., DC, United States of America South America • Belo Horizonte, Brazil • Bogota, Colombia • Buenos Aires, Argentina • Lima, Peru • Santiago, Chile • Sao Paulo, Brazil Asia Pacific • Auckland, New Zealand • Bangalore, India • Bangkok, Thailand • Beijing, China • Brisbane, Australia • Cebu City, Philippines • Gandhinagar, India • Gurgaon, India • Hanoi, Vietnam • Hong Kong, Hong Kong • Hyderabad, India • Kuala Lumpur, Malaysia • Manila, Philippines • Melbourne, Australia • Mumbai, India • New Taipei City, Taiwan • Osaka, Japan • Perth, Australia • Pune, India • Quezon City, Philippines • Seoul, South Korea • Shanghai, China • Shenzhen, China • Singapore, Singapore • South Jakarta, Indonesia • Sydney, Australia • Taipei, Taiwan • Taoyuan, Taiwan

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		• Tokyo, Japan • Zhubei City, Taiwan EMEA • Amsterdam, The Netherlands • Athens, Greece • Barcelona, Spain • Berlin, Germany • Brussels, Belgium • Bucharest, Romania • Budapest, Hungary • Copenhagen, Denmark • Doha, Qatar • Dubai, United Arab Emirates • Dublin, Ireland • Espoo, Finland • Frankfurt, Germany • Gdansk, Poland • Ghent, Belgium • Haifa, Israel • Hamburg, Germany • Helsinki, Finland • Istanbul, Turkey • Krakow, Poland • Lisbon, Portugal • London, United Kingdom • Madrid, Spain • Malaga, Spain • Manchester, United Kingdom • Milan, Italy • Munich, Germany • Oslo, Norway • Ottignies-Louvain-la-Neuve, Belgium • Paris, France • Prague, Czech Republic • Ramat Gan, Israel • Rome, Italy • Riyadh, Saudi Arabia • Stockholm, Sweden • Tel Aviv, Israel • Viby, Denmark • Vienna, Austria • Vilnius, Lithuania • Warsaw, Poland • Wroclaw, Poland • Zagreb, Croatia • Zurich, Switzerland Africa • Accra, Ghana • Cairo, Egypt • Johannesburg, South Africa

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

		• Lagos, Nigeria • Nairobi, Kenya

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

bernard@bottlebaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☐ Yes ☒ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	Description of Services Provided:
Ascenty	Colocation Data Center
Cologix	Colocation Data Center
CyrusOne	Colocation Data Center
Databank	Colocation Data Center
DigitalRealty	Colocation Data Center
Equinix	Colocation Data Center
Global Data Centers / Edgeconnex	Colocation Data Center
GreenDC	Colocation Data Center
GTD	Colocation Data Center
Macquarie	Colocation Data Center
NetMagic	Colocation Data Center
Noovle	Colocation Data Center
QTS	Colocation Data Center
SDS Data	Colocation Data Center
Sify	Colocation Data Center
Virtus	Colocation Data Center

Note: *Requirement 12.8 applies to all entities in this list.*

bernard@bomaker.ro

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD
Google Confidental Information

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	☒	☒	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐
Requirement 4:	☐	☒	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☒	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐
Requirement 12:	☒	☐	☐	☐	☐
Appendix A1:	☒	☐	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.4, 1.4.4, 3.2.1, 3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.2, 3.4.1, 3.4.2, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3, 3.6.1, 3.6.1.2, 3.7.1, 3.7.2, 3.7.3, 3.7.5, 4.1.1, 4.1.2, 4.2.1, 4.2.1.1, 4.2.1.2, 4.2.2, 6.5.5, 7.2.6, 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7, 10.2.1.1 – GCP does not store, process, or transmit account data. 2.3.1, 2.3.2 – GCP does not have wireless environments in scope for this assessment. 3.3.3 – GCP is not an issuer nor a support issuing services. 3.6.1.3, 3.7.6 – GCP does not use cleartext cryptographic key components. 3.7.8 – GCP does not manually manage keys. 3.7.9 – GCP does not share cryptographic keys with their customers for transmission or storage of account data. 5.3.2.1 – GCP uses real-time continuous behavioral analysis. 6.4.3, 11.6.1 – GCP does not have any payment pages in scope. 6.5.2, 11.3.1.3, 11.3.2.1 –GCP had no significant changes during the assessment period. 8.2.3 – GCP does not have remote access to customer premises. 8.2.7 – GCP does not allow any vendors to access their environment remotely. 8.3.10, 8.3.10.1 – GCP does not provide non-consumer access to the production environment. 8.6.1, 8.6.2 – GCP does not allow interactive login on accounts used by systems or applications. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3, A2.1.1, A2.1.2, A2.1.3 – GCP does not own or operate any point-of-sale systems.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	07/25/2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	11/30/2024
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated 12/09/2024.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)**:***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby Google LLC (Google Cloud Platform) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby Not Applicable has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: Not Applicable An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby Not Applicable has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met
Not Applicable	Not Applicable

leonardo@bomaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

DocuSigned by:
CA2DF0510F34486...

Signature of Service Provider Executive Officer ↗	Date: 12/16/2024
Service Provider Executive Officer Name: **Jeanette Manfra**	Title: **Senior Director, Global Risk and Compliance (Cloud CISO)**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed: Not Applicable

Signed by:
David Miller
5982E267E874455...

Signature of Lead QSA ↗	Date: 12/16/2024
Lead QSA Name: **David Miller**	

Signed by:
Humberto Zepeda
A1A363D2DA834A1...

Signature of Duly Authorized Officer of QSA Company ↗	Date: 12/16/2024
Duly Authorized Officer Name: **Humberto Zepeda**	QSA Company: **Coalfire Systems, Inc**

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☒ ISA(s) provided other assistance. If selected, describe all role(s) performed: ISA (Joe Nangle) assisted in the collection of assessment evidence and

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD

Google Confidental Information

	demonstrations of PCI DSS controls implementation on behalf of GCP

bernard@botmaker.io

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: E34BE435-2CF0-4A57-8D8B-B7DABA8E27BD
Google Confidental Information

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

bernard@hotmaker.io

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Google Confidental Information

COALFIRE CONTROLS

Report on Google LLC's Description of Its Internal Control System Related to Google LLC's Google Cloud Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to *Cloud Computing Compliance Criteria Catalogue (C5)* Throughout the Period April 1, 2024 to March 31, 2025

bernard@bitmaker.io

Google

Table of Contents

Section 1

Independent Service Auditor's Report 3

Section 2

Assertion of Google LLC Management 7

Section 3

Description of the Internal Control System Related to Google LLC's Google Cloud Platform Throughout the Period April 1, 2024 to March 31, 2025 10

Section 4

Presentation of Objectives, Basic Criteria, Assigned Controls, Service Auditor's Tests and Results of Tests 61

Section 5

Other Information Provided by Google LLC 295

bernard@botmaker.io

Section 1

Independent Service Auditor’s Report

bernard@botmaker.io

COALFIRE CONTROLS

Independent Service Auditor's Report

To: Google LLC ("Google")

Scope

We have examined Google's "Description of the Internal Control System Related to Google LLC's Google Cloud Platform Throughout the Period April 1, 2024 to March 31, 2025" (system description) and the suitability of the design and operating effectiveness of controls included in the description to meet the criteria set forth in the *Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Criteria Catalogue (C5)* (C5:2020), for the period April 1, 2024 to March 31, 2025. Google's management is responsible for the adequate design and operating effectiveness of the controls and compliance with the C5 basic criteria. Our responsibility is to express an opinion on the system description and on the design and operating effectiveness of these controls throughout the period April 1, 2024 to March 31, 2025, and Google's compliance with the C5 basic criteria based on our examination.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Google, to achieve the applicable C5 criteria. The description presents Google's controls, the applicable C5 criteria, and the complementary user entity controls assumed in the design of Google's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Google uses subservice organizations to provide data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Google, to achieve the applicable C5 criteria. The description presents Google's controls, the applicable C5 criteria, and the types of complementary subservice organization controls assumed in the design of Google's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by Google LLC," is presented by Google's management to provide additional information and is not a part of Google's description of its internal control system related to Google LLC's Google Cloud Platform during the period April 1, 2024 to March 31, 2025. Information included in Section 5 has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

Google is responsible for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Google's controls were designed and operating effectively to meet the C5 criteria. In Section 2, Google has provided the accompanying assertion titled "Assertion of Google LLC Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Google is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable C5 criteria and stating the related controls in the description; and identifying the risks that threaten the ability of the service organization to meet the C5 criteria commitments and system requirements.

boilerplate.io

Google Confidental Information

Service Auditor's Responsibilities

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and in accordance with International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information,* issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether Google's controls were designed and operating effectively to comply with the criteria, in all material respects. An examination involves performing procedures to obtain evidence about the design and operating effectiveness of the Company's controls and their compliance with the C5 criteria. The nature, timing and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of the design and operating effectiveness of controls in accordance with the C5 criteria, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants. Our engagement team included members with 3 years relevant professional experience with IT audits in a public audit firm.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

Because of inherent limitations, controls may not prevent, detect or correct errors or fraud which may occur. Also, projections of any evaluation of adequate design and operating effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may become inadequate or fail.

Opinion

In our opinion:

- The description fairly presents Google's internal control system related to its Google Cloud Platform to meet the applicable C5 criteria throughout the period April 1, 2024 to March 31, 2025 and includes the minimum content as set forth in Section 3.4.4.1 of the C5 Catalogue;
- The controls stated in Google's description of its Google Cloud Platform were suitably designed and implemented to meet the applicable C5 criteria throughout the period April 1, 2024 to March 31, 2025, if the subservice organizations and user entities applied the complementary controls assumed in the design of Google's controls throughout that period; and
- The controls stated in Google's description of its Google Cloud Platform operated effectively throughout the period April 1, 2024 to March 31, 2025, if complementary subservice organization controls and complementary user entity controls assumed in the design of Google's controls operated effectively throughout that period.

Restricted Use

This report is intended solely for the information and use of Google and its customers, prospective customers or regulators and is not intended to be and should not be used by anyone other than these

bernard@bormaker.io

specified parties. If a report recipient is not a specified party and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Coalfire Controls, LLC as a result of such access. Further, Coalfire Controls, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

General Terms of the Engagement

The terms of the engagement were outlined in a Statement of Work and engagement letter between Google LLC and the Service Auditor.

Coalfire Controls LLC

Greenwood Village, Colorado
June 11, 2025

bernard@botmaker.io

Section 2

Assertion of Google LLC Management

bernard@botmaker.io

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

650 253-0000 main
Google.com

Assertion of Google LLC (“Google”) Management

We have designed and documented in the description of Google LLC’s Google Cloud Platform, the internal controls of Google to comply with the criteria set forth in *Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Criteria Catalogue* (C5) (C5:2020). Our controls address the applicable basic criteria under the following objectives of C5:

- 5.1: Organisation of Information Security (OIS)
- 5.2: Security Policies and Instructions (SP)
- 5.3: Personnel (HR)
- 5.4: Asset Management (AM)
- 5.5: Physical Security (PS)
- 5.6: Operations (OPS)
- 5.7: Identity and Access Management (IDM)
- 5.8: Cryptography and Key Management (CRY)
- 5.9: Communication Security (COS)
- 5.10: Portability and Interoperability (PI)
- 5.11: Procurement, Development, and Modification of Information Systems (DEV)
- 5.12: Control and Monitoring of Service Providers and Suppliers (SSO)
- 5.13: Security Incident Management (SIM)
- 5.14: Business Continuity Management (BCM)
- 5.15: Compliance (COM)
- 5.16: Dealing with Investigation Requests from Government Agencies (INQ)
- 5.17: Product Safety and Security (PSS)

The C5 basic criteria under the objective listed below were determined not to be applicable to Google Cloud Platform, as it does not use traditional backup and recovery mechanisms and achieves data redundancy through replication across multiple clusters within Cloud Regions. This removes the need for traditional backup monitoring or recovery testing mechanisms.

- 5.6: Operations (OPS) criteria OPS-06, OPS-07 and OPS-08

bernard@botmaker.co

We confirm, to the best of our knowledge and belief, that:

- The description fairly presents Google's internal control system related to its Google Cloud Platform to meet the applicable C5 criteria throughout the period April 1, 2024 to March 31, 2025 and includes the minimum content as set forth in Section 3.4.4.1 of the C5 Catalogue;
- The controls stated in the description were suitably designed and implemented to meet the applicable C5 criteria throughout the period April 1, 2024 to March 31, 2025, if the subservice organizations and user entities applied the complementary controls assumed in the design of Google's controls throughout that period; and
- The controls stated in the description were suitably designed and operated effectively throughout the period April 1, 2024 to March 31, 2025, if complementary subservice organization controls and complementary user entity controls assumed in the design of Google's controls operated effectively throughout that period.

Google LLC

bernard@botmaker.io

Section 3

Description of the Internal Control System Related to Google LLC's Google Cloud Platform Throughout the Period April 1, 2024 to March 31, 2025

bernard@bottmaker.io

Type of Services Provided

Google LLC (“Google” or “the Company”), a subsidiary of Alphabet Inc., is a global technology service provider focused on improving the ways people connect with information. Google’s innovations in web search and advertising have made its website one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world’s largest online indexes of websites and other content and makes this information freely available to anyone with an Internet connection. Google’s automated search technology helps people obtain nearly instant access to relevant information from their vast online index.

Google Cloud Platform provides infrastructure-as-a-service (IaaS), software-as-a-service (SaaS), and platform-as-a-service (PaaS), allowing businesses and developers to build and run any or all of their applications on Google’s cloud infrastructure. Customers can benefit from the performance, scale, reliability, ease of use, and a pay-as-you-go cost model.

Google’s product offerings for Google Cloud Platform allow customers to leverage the resources of Google’s core Engineering team, as well as a team dedicated to developing solutions for the corporate market. As a result, these Google offerings are positioned to innovate at a rapid rate and provide the same level of service that users are familiar with on google.com.

Google Cloud Platform includes the following services, hereafter described collectively as “Google Cloud Platform” or “GCP”:

- Artificial Intelligence (AI) and Machine Learning (ML): Innovative, scalable ML services, with pretrained models and the ability to generate tailored models
- Application Programming Interface (API) Management: Developing, deploying, and managing APIs on any Google Cloud back end
- Compute: A range of computing options tailored to match the size and needs of any organization
- Data Analytics: Tools to capture, process, store, and analyze data on a single platform
- Databases: Migrating, managing, and modernizing data with secure, reliable, and highly available relational and nonrelational databases that allow for the migration, management, and modernization of data
- Developer Tools: A collection of tools and libraries that help development teams work more quickly and effectively
- Healthcare and Life Sciences: Healthcare solution to protect sensitive data and maintain compliance with numerous requirements across various domains, geographies, and workloads
- Hybrid and Multi-cloud: Connecting on-premises or existing cloud infrastructure with Google Cloud’s scalability and innovation
- Management Tools: Managing applications on GCP with a web-based console, mobile application, or Cloud Shell for real-time monitoring, logging, diagnostics, and configuration
- Media and Gaming: Building user experiences and empowering developers by minimizing infrastructure complexity and accelerating data insights
- Migration: Large-scale, secure online data transfers to Google Cloud Storage and databases
- Networking: A private network using software-defined networking and distributed systems technologies to host and deliver services around the world

bernard@betmaker.io

- Operations: Suite of products to monitor, troubleshoot, and improve application performance on Google Cloud environments
- Security and Identity: Managing the security and access to cloud assets, supported by Google's own protection of its infrastructure
- Serverless Computing: Deploying functions or applications as source code or as containers without worrying about the underlying infrastructure, and building full-stack serverless applications with Google Cloud's storage, databases, ML, and more
- Storage: Scalable storage options and varieties for different needs and price points
- Other: Additional GCP services supporting e-commerce, procurement, billing, and petabyte-scale scientific analysis and visualization of geospatial datasets

The Google Cloud Platform products covered in this system description consist of the following services:

- Artificial Intelligence (AI) and Machine Learning (ML)
  - Agent Assist
  - AI Platform Deep Learning Container
  - AI Platform Neural Architecture Search (NAS)
  - AI Platform Training and Prediction
  - Anti-Money Laundering (AML) AI
  - AutoML Tables
  - AutoML Translation
  - Cloud Natural Language API
  - Cloud Speaker ID
  - Cloud Translation
  - Cloud Vision
  - Conversational AI (formerly Contact Center AI (CCAI))
  - Conversational Insights (formerly Contact Center AI Insights)
  - Dialogflow
  - Discovery Solutions
  - Document AI
  - Document AI Warehouse
  - Food Ordering AI Agent
  - Gemini for Google Cloud
  - Generative AI on Vertex AI
  - Google Cloud Contact Center as a Service (CCaaS)
  - Ray on Vertex AI
  - Recommendations AI
  - Retail Search
  - Speech-to-Text
  - Talent Solution

bernard@botmaker.io

  - Text-to-Speech
  - Vertex AI Codey
  - Vertex AI Colab Enterprise
  - Vertex AI Conversation
  - Vertex AI Platform
  - Vertex AI Search
  - Vertex AI Workbench Instances
  - Video Intelligence API
- Application Programming Interface (API) Management
  - Advanced API Security
  - Apigee
  - API Gateway
  - Application Integration
  - Cloud Endpoints
  - Integration Connectors
- Compute
  - App Engine
  - Batch
  - Compute Engine
  - Workload Manager
- Data Analytics
  - BigQuery
  - BigQuery Omni[1]
  - Cloud Composer
  - Cloud Data Fusion
  - Cloud Life Sciences
  - Data Catalog
  - Dataflow
  - Dataform
  - Dataplex
  - Dataproc
  - Dataproc Metastore
  - Looker (Google Cloud core)
  - Looker Studio

bernard@botmaker.io

[1] BigQuery Omni is a Google-Managed Multi-Cloud Service as per Google Cloud Platform Services Summary (https://cloud.google.com/terms/services) (as of the date of this report).

Google Confidental Information

  - Managed Service for Apache Kafka
  - Pub/Sub
- Databases
  - AlloyDB
  - Cloud Bigtable
  - Cloud Spanner
  - Cloud SQL
  - Datastore
  - Firestore
  - Memorystore
- Developer Tools
  - Artifact Analysis
  - Artifact Registry
  - Cloud Build
  - Cloud Source Repositories
  - Cloud Workstations
  - Container Registry
  - Firebase Test Lab
  - Google Cloud Deploy
  - Google Cloud SDK
  - Infrastructure Manager
  - Secure Source Manager
- Healthcare and Life Sciences
  - Cloud Healthcare
  - Healthcare Data Engine (HDE)
- Hybrid and Multi-cloud
  - Connect
  - Google Kubernetes Engine (GKE)
  - GKE Enterprise Config Management
  - GKE Identity Service
  - Hub
  - Knative serving
  - Service Mesh
- Management Tools
  - Cloud Console
  - Cloud Console App
  - Cloud Deployment Manager

bernard@botmaker.io

  - Cloud Shell
  - Recommender
  - Service Infrastructure
- Media and Gaming
  - Media CDN
  - Transcoder API
- Migration
  - BigQuery Data Transfer Service
  - Database Migration Service
  - Migration Center
  - Migrate to Virtual Machines
  - Storage Transfer Service
- Networking
  - Cloud CDN
  - Cloud DNS
  - Cloud IDS (Cloud Intrusion Detection System)
  - Cloud Interconnect
  - Cloud Load Balancing
  - Cloud Network Address Translation (NAT)
  - Cloud Next Generation Firewall (NGFW)
  - Cloud Router
  - Cloud Service Mesh
  - Cloud Virtual Private Network (VPN)
  - Google Cloud Armor
  - Network Connectivity Center
  - Network Intelligence Center
  - Network Service Tiers
  - Service Directory
  - Spectrum Access System
  - Traffic Director
  - Virtual Private Cloud (VPC)
- Operations
  - Cloud Logging
  - Cloud Monitoring
  - Cloud Profiler
  - Cloud Trace
  - Google Cloud Backup and Disaster Recovery (DR)

bernard@botmaker.io

  - Personalized Service Health
- Security and Identity
  - Access Approval
  - Access Context Manager
  - Access Transparency
  - Assured Workloads
  - Binary Authorization
  - Certificate Authority Service
  - Certificate Manager
  - Chrome Enterprise Premium
  - Cloud Asset Inventory
  - Cloud External Key Manager (Cloud EKM)
  - Cloud Hardware Security Module (HSM)
  - Cloud Key Management Service
  - Firebase App Check
  - Firebase Authentication
  - Google Cloud Identity-Aware Proxy (IAP)
  - Google Security Operations (SIEM)[2]
  - Google Security Operations (SOAR)[2]
  - Google Threat Intelligence[2]
  - Identity and Access Management (IAM)
  - Identity Platform
  - Key Access Justifications (KAJ)
  - Managed Service for Microsoft Active Directory (AD)
  - Organization Policy
  - Privileged Access Manager
  - reCAPTCHA Enterprise
  - Resource Manager API
  - Risk Manager
  - SecLM
  - Secret Manager
  - Security Command Center
  - Sensitive Data Protection (including Cloud Data Loss Prevention)
  - VirusTotal

bernard@botmaker.io

[2] Google Security Operations SIEM, Google Security Operations SOAR and Google Threat Intelligence for Google Security Operations are covered by separate terms than GCP. Refer to the Terms of Service (https://cloud.google.com/terms/secops/service-terms) (as of the date of this report) for additional details.

Google Confidental Information

  - VPC Service Controls
  - Web Risk API
- Serverless Computing
  - Cloud Functions
  - Cloud Functions for Firebase
  - Cloud Run
  - Cloud Scheduler
  - Cloud Tasks
  - Datastream
  - Eventarc
  - Workflows
- Storage
  - Backup for GKE
  - Cloud Filestore
  - Cloud Storage
  - Cloud Storage for Firebase
  - Parallelstore
  - Persistent Disk
- Other
  - Cloud Billing
  - Google Earth Engine
  - Google Cloud Marketplace
  - Google Cloud Skills Boost
  - Google Cloud VMware Engine (GCVE)
  - Tables

bernard@botmaker.io

The products are composed of communication, productivity, collaboration, and security tools that can be accessed from virtually any location that has secure Internet connectivity. This means every employee and each user entity they work with can be productive from anywhere, using any device with a secure Internet connection.

These products provide a comprehensive variety of technical services that organizations rely on. See the subsections below for more information on each.

Artificial Intelligence and Machine Learning

Google does not use customer data to train or fine-tune any AI or ML models without a customer's prior permission or instruction. Refer to the service terms (https://cloud.google.com/terms/service-terms) (as of the date of this report) for additional details.

Agent Assist

Agent Assist is a large language model (LLM)-powered AI solution that increases human agent productivity and enhances customer service by offering real-time assistance.

AI Platform Deep Learning Container

AI Platform Deep Learning Container provides Docker images with AI frameworks that can be customized and used with GKE, Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.

AI Platform Neural Architecture Search

AI Platform NAS is a managed service leveraging Google's neural architecture search technology to generate, evaluate, and train numerous model architectures for a customer's application. AI Platform NAS training services facilitate management of large-scale experiments.

AI Platform Training and Prediction

AI Platform Training and Prediction is a managed service that enables users to easily build ML models with popular frameworks like TensorFlow, XGBoost, and Scikit Learn. It provides scalable training and prediction services that work on large datasets.

Anti-Money Laundering AI

AML AI is an ML engine that uses customer data and training labels to create a tailored model covering an extensible typology of risks for AML, along with governance documentation to ease adoption in this highly regulated environment.

AutoML Tables

AutoML Tables enables data scientists, analysts, and developers to automatically build and deploy ML models on structured data at increased speed and scale.

AutoML Translation

AutoML Translation is a simple and scalable translation solution that allows businesses and developers with limited ML expertise to customize the Google Neural Machine Translation model for their own domain or use-case.

Cloud Natural Language API

Cloud Natural Language API provides natural language understanding as a simple-to-use API. Given a block of text, this API enables finding entities, analyzing sentiment (positive or negative), analyzing syntax (including parts of speech and dependency trees), and categorizing the content into a rich taxonomy. The API can be called by passing the content directly or by referring to a document in Cloud Storage.

Cloud Speaker ID

Speaker ID allows customers to enroll user voice prints and later verify users against a previously enrolled voice print.

Cloud Translation

Cloud Translation automatically translates text from one language to another language (e.g., French to English). The API is used to programmatically translate text in webpages or applications.

bernard@botmaker.io

Cloud Vision

Cloud Vision enables the understanding of image content by encapsulating ML models in a Representational State Transfer (REST) API. It classifies images into thousands of categories, detects individual objects and faces within images, and finds and reads printed words contained within images. It can be applied to build metadata on image catalogs, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. It can also analyze images uploaded in the request and integrate with image storage on Google Cloud Storage.

Conversational AI (formerly Contact Center AI (CCAI))

Conversational AI uses AI to improve the customer experience in contact centers. It includes Agent Assist, Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Insights, Speech-to-Text, Text-to-Speech, and Speaker ID.

Conversational Insights (formerly Contact Center AI Insights)

Conversational Insights helps customers extract value from their contact center data by identifying sentiment and topics and highlighting key insights in the data.

Dialogflow

Dialogflow is a development suite for voice and text conversational applications, including chatbots. Dialogflow is cross-platform and can connect to applications on the web, Android, iOS, and IoT or on existing platforms (e.g., Actions on Google, Facebook Messenger, Slack).

Discovery Solutions

Discovery Solutions enable customers in retail, media, and other verticals to deliver Google-quality search results and recommendations.

Document AI

Document AI classifies and extracts structured data from documents to help streamline data validation and automate business processes.

Document AI Warehouse

Document AI Warehouse is a data management and governance platform that stores, searches, and organizes documents and their extracted and tagged metadata. Document AI Warehouse is highly scalable and fully managed and can be integrated with enterprise document workflows, applications, and repositories.

Food Ordering AI Agent

Food Ordering AI Agent is a repeatable, scalable food ordering voice assistant that helps restaurants serve their customers with high quality and consistent service.

Google Cloud Contact Center as a Service (CCaaS) (formerly Contact Center AI Platform)

Google Cloud CCaaS is a contact-center-as-a-service (CCaaS) platform leveraging Conversational AI. It integrates directly with CRMs and queues and routes customer interactions across voice and digital channels to resource pools, including human agents.

Gemini for Google Cloud

Gemini for Google Cloud provides AI-powered end user assistance with a wide range of Google Cloud products. Gemini for Google Cloud is a generative AI-powered collaboration Service that provides

gernard@botmaker.io

assistance to Google Cloud end users. Gemini for Google Cloud is embedded in many Google Cloud products to provide developers, data scientists, and operators an integrated assistance experience.

Generative AI on Vertex AI

Generative AI on Vertex AI includes features for generative AI use cases, including LLMs and text-to-image and image-to-text models.

Ray on Vertex AI

Ray on Vertex AI is an open-source framework for scaling AI and Python applications. Ray provides the infrastructure to perform distributed computing and parallel processing for clients' ML workflows.

Recommendations AI

Recommendations AI enables customers to build a personalized recommendation system using ML models.

Retail Search

Retail Search allows retailers to leverage Google's search capabilities on their retail websites and applications.

Speech-to-Text

Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy-to-use API.

Talent Solution

Talent Solution offers access to Google's ML, enabling company career sites, job boards, application tracking systems, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.

Text-to-Speech

Text-to-Speech synthesizes human-like speech based on input text in a variety of voices and languages.

Vertex AI Codey

Vertex AI Codey generates code based on natural language input. Good for writing functions, classes, unit tests, and more.

Vertex AI Colab Enterprise

Vertex AI Colab Enterprise is a collaborative, managed notebook environment with the security and compliance capabilities of Google Cloud.

Vertex AI Conversation

Vertex AI Conversation allows customers to leverage foundational models and conversational AI to create multimodal chat or voice agents.

Vertex AI Platform

Vertex AI Platform is a service for managing the AI and ML development lifecycle. Customers can (i) store and manage datasets, labels, features, and models; (ii) build pipelines to train and evaluate models and run experiments using Google Cloud algorithms or custom training code; (iii) deploy models for online or

bernard@botmaker.io

batch use cases; (iv) manage data science workflows using Colab Enterprise and Vertex AI Workbench (also known as Notebooks); and (v) create business optimization plans with Vertex Decision Optimization.

Vertex AI Search

Vertex AI Search allows customers to leverage foundational models and search and recommendation technologies to create multimodal semantic search and question-answering experiences.

Vertex AI Workbench Instances

Vertex AI Workbench instances are Jupyter Notebook–based development environments for the entire data science workflow. You can interact with Vertex AI and other Google Cloud services from within a Vertex AI Workbench instance's Jupyter Notebook.

Video Intelligence API

Video Intelligence API makes videos searchable and discoverable by extracting metadata through a REST API. It annotates videos stored in Google Cloud Storage and helps identify key noun entities in a video and when they occur within the video.

API Management

Advanced API Security

Advanced API Security constantly analyzes incoming traffic, seeking out anomalous patterns that might indicate attacks or abuse. When suspicious activity is spotted, it can block harmful requests or alert users for further action. Additionally, it evaluates a user's API setups against security best practices, offering recommendations for improvement. This comprehensive approach helps users proactively safeguard their APIs, protect sensitive data, and ensure their API configurations are designed to withstand security challenges.

Apigee

Apigee is a full-lifecycle API management platform that lets customers design, secure, analyze, and scale APIs, giving them visibility and control. Apigee is available as Apigee, a fully managed service; Apigee hybrid, a hybrid model that is partially hosted and managed by the customer; or Apigee Private Cloud, an entirely customer-hosted premium software solution. Apigee Private Cloud is not in scope for this report.

API Gateway

API Gateway is a fully managed service that enables users to develop, deploy, and secure APIs running on Google Cloud Platform.

Application Integration

Application Integration is an integration-platform-as-a-service (iPaaS) that offers a comprehensive set of integration tools to connect and manage the multitude of applications and data required to support various business operations. Application Integration provides a unified drag-and-drop integration designer interface, triggers that help invoke an integration, configurable tasks and numerous connectors that allow connectivity to business applications, technologies, and other data sources using the native protocols of each target application.

Cloud Endpoints

Cloud Endpoints is a tool that provides services to develop, deploy, secure, and monitor APIs running on Google Cloud Platform.

bernard@hotmaker.ro

Integration Connectors

Integration Connectors is a platform that allows customers to connect to business applications, technologies, and other data sources using native protocols of each target application. The connectivity established through these connectors helps manage access to various data sources, which can be used with other services like Application Integration through a consistent, standard interface.

Compute

App Engine

App Engine enables the building and hosting of web applications on the same systems that power Google applications. App Engine offers fast development and deployment of applications without the need to manage servers or other low-level infrastructure components. Scaling and software patching are managed by App Engine on the user's behalf. App Engine also provides the ability to create managed virtual machines (VMs). In addition, client APIs can be built for App Engine applications using Google Cloud Endpoints.

Batch

Batch is a fully managed service that lets users schedule, queue, and execute batch processing workloads on Compute Engine VM instances. Batch provisions resources and manages capacity on users' behalf, allowing user batch workloads to run at scale.

Compute Engine

Compute Engine offers scalable and flexible VM computing capabilities in the cloud. With VMs that can boot in minutes, it offers many configurations, including custom machine types that can be optimized for specific use cases as well as support for graphics processing units (GPUs), tensor processing units (TPUs), and local solid-state drive (SSD). Additionally, customers can enable Shielded VMs to provide advanced platform security.

Workload Manager

Workload Manager is a rule-based validation service for evaluating workloads running on Google Cloud. If enabled, Workload Manager scans application workloads to detect deviations from standards, rules, and best practices that improve system quality, reliability, and performance.

Data Analytics

BigQuery

BigQuery is a fully managed, petabyte-scale analytics data warehouse that features scalable data storage and the ability to perform ad hoc queries on multi-terabyte datasets. BigQuery allows users to share data insights via the web and control access to data based on business needs.

BigQuery Omni

BigQuery Omni is a flexible, multi-cloud analytics solution, powered by Anthos, that allows users to analyze data across cloud platforms. BigQuery Omni uses standard SQL and BigQuery's familiar interface to quickly answer questions and share results from a single pane of glass across datasets.

BigQuery Omni is a Google-Managed Multi-Cloud Service as per Google Cloud Platform Services Summary (https://cloud.google.com/terms/services) (as of the date of this report).

bernard@hotmaker.io

Google Cloud Platform uses Amazon Web Services (AWS) and Microsoft Azure (Azure) as subservice organizations (internally referred to as “Multi-Cloud Service Third-Party Providers”) for cloud-based hosting services for Google-Managed Multi-Cloud Services.

Cloud Composer

Cloud Composer is a managed workflow orchestration service that can be used to author, schedule, and monitor pipelines that span clouds and on-premises data centers.

Cloud Data Fusion

Cloud Data Fusion is a fully managed, cloud-native enterprise data integration service for building and managing data pipelines. Cloud Data Fusion provides a graphical interface that allows customers to build scalable data integration solutions to cleanse, prepare, blend, transfer, and transform data.

Cloud Life Sciences

Cloud Life Sciences is a suite of services and tools to store, process, inspect, and share biomedical data, DNA sequence reads, reference-based alignments, and variant calls using Google’s cloud infrastructure.

Data Catalog

Data Catalog is a fully managed and scalable metadata management service that allows organizations to have a centralized and unified view of data assets.

Dataflow

Dataflow is a fully managed service for consistent, parallel data-processing pipelines. It utilizes the Apache Beam software development kits (SDKs) with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the lifecycle of Compute Engine resources for the processing pipeline(s) and provides a monitoring interface for understanding pipeline health.

Dataform

Dataform is a service for data analysts to develop, test, version control, and schedule complex SQL workflows for data transformation in BigQuery. Dataform lets users manage data transformation in the extract, load, and transform (ELT) process for data integration. After raw data is extracted from source systems and loaded into BigQuery, Dataform helps users to transform it into a well-defined, tested, and documented suite of data tables.

Dataplex

Dataplex is an intelligent data fabric that helps customers unify distributed data and automate management and governance across that data to power analytics at scale.

Dataproc

Dataproc is a managed service for distributed data processing. It provides management, integration, and development tools for deploying and using Apache Hadoop, Apache Spark, and other related open-source data processing tools. With Dataproc, clusters can be created and deleted on demand and sized to fit any workload.

Dataproc Metastore

Dataproc Metastore provides a fully managed metastore service that simplifies technical metadata management and is based on a fully featured Apache Hive metastore. Dataproc Metastore can be used as

vedran@otmaker.io

a metadata storage service component for data lakes built on open-source processing frameworks (e.g., Apache Hadoop, Apache Spark, Apache Hive, Presto).

Looker (Google Cloud core)

Looker (Google Cloud core) is a business intelligence and embedded analytics solution hosted on Google infrastructure. With Looker (Google Cloud core), customers can build semantic models using various data sources, develop customized insights from the models, and share those insights for collaboration via dashboards and other services.

Looker Studio

Looker Studio is a visualization and business intelligence product that enables users to connect to multiple datasets and turn their data into informative, easy-to-share, and fully customizable dashboards and reports.

Managed Service for Apache Kafka

Managed Service for Apache Kafka is a Google Cloud service that helps you run secure, scalable open-source Apache Kafka clusters.

Pub/Sub

Pub/Sub provides reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a topic while other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Pub/Sub allows communication between independent applications.

Databases

AlloyDB

AlloyDB is an enterprise-grade database product that combines the familiarity of open-source database front ends, like PostgreSQL, with custom-built storage, query, and connectivity layers for increased availability, performance, security, and manageability.

Cloud Bigtable

Cloud Bigtable is a low-latency, fully managed, highly scalable NoSQL database service designed for the retention and serving of data from gigabytes to petabytes in size.

Cloud Spanner

Cloud Spanner is a fully managed, scalable, relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and atomicity, consistency, isolation, durability (ACID) transactions with synchronous replication of data across regions.

Cloud SQL

Cloud SQL is a service to create, configure, and use managed, third-party relational databases in GCP. Cloud SQL maintains, manages, and administers those databases.

Datastore

Datastore is a highly scalable NoSQL database for mobile and web applications, providing query capabilities, atomic transitions, and indexes, as well as automatically scaling up and down in response to load.

bernard@botmaker.io

Firestore

Firestore is a fully managed, scalable, serverless NoSQL document database for mobile, web, and server development. It provides query capabilities, live synchronization, and offline support.

Memorystore

Memorystore for Redis provides a fully managed, in-memory data store service for GCP. Memorystore can be used to build application caches that provide low-latency data access. Memorystore is compatible with the Redis protocol, allowing seamless migration with no code changes.

Developer Tools

Artifact Analysis

Artifact Analysis is a family of services that provide software composition analysis, metadata storage and retrieval. Its detection points are built into a number of Google Cloud products such as Artifact Registry and GKE for quick enablement. The service works with both Google Cloud's first-party products and also lets users store information from third-party sources. The scanning services leverage a common vulnerability store for matching files against known vulnerabilities.

Artifact Registry

Artifact Registry is a service for managing container images and packages. It is integrated with Google Cloud tooling and runtimes and comes with support for native artifact protocols, making it simple to integrate it with user continuous integration and continuous delivery (CI/CD) tooling to set up automated pipelines.

Cloud Build

Cloud Build allows for the creation of container images from application source code located in Google Cloud Storage or in a third-party service (e.g., GitHub, Bitbucket). Created container images can be stored in Container Registry and deployed on Container Engine, Compute Engine, App Engine Flexible Environment, or other services, to run applications from Docker containers.

Cloud Source Repositories

Cloud Source Repositories provides Git version control to support collaborative development of any application or service, as well as a source browser that can be used to browse the contents of repositories and view individual files from within the Cloud Console. Cloud Source Repositories and related tools (e.g., Cloud Debugger) can be used to view debugging information alongside code during application runtime.

Cloud Workstations

Cloud Workstations provides preconfigured, customizable, and secure managed development environments on Google Cloud. Cloud Workstations is accessible through a browser-based integrated development environment (IDE), from multiple local code editors (e.g., IntelliJ IDEA Ultimate, VS Code), or through Secure Shell (SSH). Instead of manually setting up development environments, users can create a workstation configuration specifying user environments in a reproducible way.

Container Registry

Container Registry is a private Docker image storage system on GCP.

Firebase Test Lab

Firebase Test Lab provides cloud-based infrastructure for testing applications on physical and virtual devices and allows developers to test their applications across a wide variety of devices.

lyenard@bomaker.io

Google Cloud Deploy

Google Cloud Deploy is a managed service that automates delivery of user applications to a series of target environments in a defined promotion sequence. When users want to deploy updated applications, they create a release whose lifecycle is managed by a delivery pipeline.

Google Cloud SDK

Google Cloud SDK is a set of tools to manage resources and applications hosted on GCP. It includes the Google Cloud Command Line Interface (CLI); Cloud Client Libraries for programmatic access to GCP services; the gsutil, kubectl, and BigQuery command line tools; and various service and data emulators for local platform development. The Google Cloud SDK provides the primary programmatic interfaces to GCP.

Infrastructure Manager

Infrastructure Manager is a managed service that automates the deployment and management of Google Cloud infrastructure resources. Infrastructure is defined using Terraform and deployed onto Google Cloud by Infrastructure Manager, enabling users to manage resources using infrastructure-as-code (IaC).

Secure Source Manager

Secure Source Manager is a fully managed service that provides a Git-based source code management system.

Healthcare and Life Sciences

Cloud Healthcare

Cloud Healthcare provides managed services and an API to store, process, manage, and retrieve healthcare data in a variety of industry-standard formats.

Healthcare Data Engine

HDE is a solution that enables (i) the harmonization of healthcare data to the Fast Healthcare Interoperability Resources (FHIR) standard and (ii) the streaming of healthcare data to an analytic environment.

Hybrid and Multi-cloud

The scope of the services included in this report is limited to the services managed by Google and does not extend to the application of the services in other cloud service providers' environments by the user entity. Refer to the Terms of Service (https://cloud.google.com/terms/services) (as of the date of this report) for additional details.

Connect

Connect is a service that allows users to connect Kubernetes clusters to the cloud, enabling both users and Google-hosted components to interact with clusters through a connection to the in-cluster Connect software agent.

Google Kubernetes Engine

Google Kubernetes Engine (GKE), powered by the open-source container scheduler Kubernetes, runs containers on GCP. GKE manages provisioning and maintaining the underlying VM cluster, scaling applications, and operational logistics such as logging, monitoring, and cluster health management.

bernard@hotmaker.io

GKE Enterprise Config Management

GKE Enterprise Config Management is a policy management solution for enabling consistent configuration across multiple Kubernetes clusters. GKE Enterprise Config Management allows customers to specify one single source of truth and then enforce those policies on the clusters.

GKE Identity Service

GKE Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple environments. Users can log in to and access their clusters from the command line or from the Cloud Console, all using their existing identity providers.

Hub

Hub is a centralized control plane that enables a user to centrally manage features and services on customer-registered clusters running in a variety of environments, including in Google's cloud, on premises in customer data centers, or in other third-party clouds.

Knative serving

Knative serving is Google's managed and fully supported Knative offering. Knative serving abstracts away the complexity of Kubernetes, making it easy to build and deploy user's serverless workloads across hybrid and multi-cloud environments.

Service Mesh

Service Mesh is a managed service mesh service that includes (i) a managed certificate authority that issues cryptographic certificates that identify customer workloads within the Service Mesh for mutual authentication, and (ii) telemetry for customers to manage and monitor their services. Customers receive details showing an inventory of services, can understand their service dependencies, and receive metrics for monitoring their services. Service Mesh is provided as a service and as a software. The Service Mesh software offering is not in scope for this report.

Management Tools

Cloud Console

Cloud Console is a web-based interface used to build, modify, and manage services and resources on GCP. Cloud services can be procured, configured, and run from Cloud Console.

Cloud Console App

Cloud Console App is a native mobile application that provides monitoring, alerting, and the ability to take actions on resources.

Cloud Deployment Manager

Cloud Deployment Manager is an infrastructure management service that automates the creation and management of GCP resources.

Cloud Shell

Cloud Shell provides command line access to GCP resources through an in-browser Linux shell backed by a temporary Linux VM in the cloud. It allows projects and resources to be managed without having to install additional tools on systems and comes equipped and configured with common developer tools such as text editors, a MySQL client, and Kubernetes.

bernard@botmaker.io

Recommender

Recommender automatically analyzes usage patterns to provide recommendations and insights across services to help a user use GCP in a more secure, cost-effective, and efficient manner.

Service Infrastructure

Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services. It includes:

- Service Management API, which lets service producers manage their APIs and services
- Service Consumer Management API, which lets service producers manage their relationships with their service consumers
- Service Control API, which lets managed services integrate with Service Infrastructure for admission control and telemetry reporting functionality
- Service Usage API, which lets service consumers manage their usage of APIs and services

Media and Gaming

Media CDN

Media CDN is a planet-scale content delivery network allowing customers to automate all facets of deployment and management. Users can stream media and deliver exceptional experiences to customer end users, no matter where they are.

Transcoder API

Transcoder API batch-converts media files into optimized formats to enable streaming across web, mobile, and living room devices. It provides fast, easy-to-use, large-scale processing of advanced codecs while utilizing Google's storage, networking, and delivery infrastructure.

Migration

BigQuery Data Transfer Service

BigQuery Data Transfer Service automates data movement from SaaS applications to BigQuery on a scheduled, managed basis.

Database Migration Service

Database Migration Service is a fully managed migration service that enables users to perform high-fidelity, minimal-downtime migrations at scale. Users can use Database Migration Service to migrate from on-premises environments, Compute Engine, and other clouds to certain Google Cloud–managed databases.

Migration Center

Migration Center provides tools, best practices, and data-driven prescriptive guidance designed to facilitate the end-to-end cloud migration journey through business case development, environment discovery, workload mapping, migration planning, financial analysis, foundation setup, and migration execution.

Migrate to Virtual Machines

Migrate to Virtual Machines is a fully managed migration service that enables customers to migrate workloads at scale into Google Cloud Compute Engine with minimal downtime by utilizing replication-based migration technology.

bernardo@botmaker.io

Storage Transfer Service

Storage Transfer Service provides the ability to import large amounts of online data into Google Cloud Storage. It can transfer data from Amazon Simple Storage Service (Amazon S3) and other HTTP/HTTPS locations, as well as transfer data between Google Cloud Storage buckets.

Networking

Cloud CDN

Cloud CDN uses Google's distributed network edge points of presence to cache HTTP(S) load-balanced content.

Cloud DNS

Cloud DNS is a fully managed Domain Name System (DNS) service that operates a geographically diverse network of high-availability, authoritative name servers. Cloud DNS provides a service to publish and manage DNS records for applications and services.

Cloud Next Generation Firewall (NGFW)

Cloud NGFW is a fully distributed, cloud-native firewall service that evaluates incoming and outgoing traffic on a network, according to user-defined firewall rules in the policy.

Cloud IDS (Cloud Intrusion Detection System)

Cloud IDS is a managed service that aids in detecting certain malware, spyware, command-and-control attacks, and other network-based threats.

Cloud Interconnect

Cloud Interconnect offers enterprise-grade connections to GCP, including providing direct connection between on-premises networks and GCP VPC.

Cloud Load Balancing

Cloud Load Balancing is a distributed, software-defined, managed service for all traffic (HTTP/HTTPS, Transmission Control Protocol (TCP)/Secure Sockets Layer (SSL), and User Datagram Protocol (UDP)) to computing resources. Cloud Load Balancing rapidly responds to changes in traffic, network, back-end health, and other related conditions.

Cloud NAT

Cloud NAT enables VM instances in a private network to communicate with the Internet without external Internet Protocol (IP) addresses.

Cloud Router

Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between a VPC network and an external network, typically an on-premises network.

Cloud Service Mesh

Cloud Service Mesh is a fully managed service mesh across all Google Cloud platform types. Cloud Service Mesh takes the Traffic Director's control plane and Google's open-source Istio-based service mesh, Anthos Service Mesh, and combines them into a single offering.

lyonard@boilmaker.io

Cloud VPN

Cloud VPN provides connections between on-premises or other external networks to VPCs on GCP via an Internet Protocol Security (IPsec) connection or can be used to connect two different Google-managed VPN gateways.

Google Cloud Armor

Google Cloud Armor provides access control configurations and at-scale defenses to help protect infrastructure and applications against distributed denial-of-service (DDoS), application-aware, and multivector attacks.

Network Connectivity Center

Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud that facilitates connecting a customer's resources to its cloud network.

Network Intelligence Center

Network Intelligence Center provides a single console for managing Google Cloud's comprehensive network monitoring, verification, and optimization platform across the Google Cloud, multi-cloud, and on-premises environments.

Network Service Tiers

Network Service Tiers enable the selection of different quality networks (tiers) for outbound traffic to the Internet: Standard Tier primarily utilizes third-party transit providers, while Premium Tier leverages Google's private backbone and peering surface for egress.

Service Directory

Service Directory is a managed service that offers customers a single place to publish, discover, and connect their services in a consistent way, regardless of their environment. Service Directory supports services in Google Cloud, multi-cloud, and on-premises environments and can scale up to thousands of services and endpoints for a single project.

Spectrum Access System

Spectrum Access System enables users to access the Citizens Broadband Radio Service (CBRS) in the United States, the 3.5 GHz band that is available for shared commercial use. Users can use Spectrum Access System to register CBRS devices, manage CBRS deployments, and access a non-production test environment.

Traffic Director

Traffic Director is GCP's traffic management service for open-source service meshes.

Virtual Private Cloud

VPC is a comprehensive set of managed networking capabilities for Google Cloud resources, including granular IP address range selection, routes, and firewalls.

Operations

Backup and DR Service

Backup and DR Service is a managed backup and disaster recovery service for centralized protection of workloads in Google Cloud.

bernard@bolmaker.io

Cloud Debugger

Cloud Debugger provides the ability to inspect the call-stack and variables of a running cloud application in real time without stopping it. It can be used in test, production, or any other deployment environment and can be used to debug applications written in supported languages.

Cloud Logging

Cloud Logging is a hosted solution that helps users gain insight into the health, performance, and availability of their applications running on GCP and other public cloud platforms. It includes monitoring dashboards to display key metrics, define alerts, and report on the health of cloud systems. The components of Cloud Logging that run on other public cloud platforms are not in scope for this report.

Cloud Monitoring

Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from certain services, hosted uptime probes, application instrumentation, alert management, notifications, and a variety of application components.

Cloud Profiler

Cloud Profiler continuously gathers and reports source-level performance information from production services. It provides key information to determine what functions in code consume the most memory and central processing unit (CPU) cycles, enabling insight into how code operates to improve performance and optimize computing resources.

Cloud Trace

Cloud Trace collects latency data from applications and displays it in the GCP Console. It automatically analyzes trace data to generate in-depth performance reports that help identify and locate performance bottlenecks.

Personalized Service Health

Personalized Service Health lets users identify Google Cloud service disruptions relevant to their projects so they can manage and respond to them efficiently. These disruptions are called service health events and are available in the Google Cloud console and a variety of integration points.

bernard@bottmaker.io

Security and Identity

Access Approval

Access Approval allows customers to approve eligible manual, targeted access by Google administrators to their data or workloads prior to access being granted.

Access Context Manager

Access Context Manager allows customer administrators to define attribute-based access control for projects, applications, and resources.

Access Transparency

Access Transparency captures near-real-time logs of certain manual, targeted accesses by Google personnel and provides them via Cloud Logging accounts.

Assured Workloads

Assured Workloads provides functionality to create security controls that are enforced on a customer cloud environment and can assist with compliance requirements (e.g., FedRAMP Moderate compliance).

Binary Authorization

Binary Authorization helps customers ensure that only signed and explicitly authorized container images are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.

Certificate Authority Service

Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Customers can use Certificate Authority Service to create certificate authorities using Cloud Key Management Service keys to issue, revoke, and renew subordinate and end-entity certificates.

Certificate Manager

Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the certificates.

Chrome Enterprise Premium (formerly BeyondCorp Enterprise)

Chrome Enterprise Premium is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware, and phishing attacks. Chrome Enterprise Premium is an integrated platform incorporating cloud-based services and software components.

Cloud Asset Inventory

Cloud Asset Inventory is a service that allows customers to view, monitor, and analyze cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.

Cloud External Key Manager

Cloud EKM lets customers encrypt data in GCP with encryption keys that are stored and managed in a third-party key management system deployed outside Google’s infrastructure.

Cloud Hardware Security Module

Cloud HSM is a cloud-hosted hardware security module service for hosting encryption keys and performing cryptographic operations.

Cloud Key Management Service

Cloud Key Management Service is a cloud-hosted key management service that manages encryption for cloud services. It enables the generation, use, rotation, and destruction of encryption keys.

Firebase App Check

Firebase App Check provides a service that can help protect access to users' APIs with platform-specific attestation that helps verify application identity and device integrity.

Firebase Authentication

Firebase Authentication is a fully managed user identity and authentication system providing back-end services enabling sign-in and sign-up experiences for an application or service.

bernard@bdmaker.io

Google Cloud Identity-Aware Proxy

Google Cloud IAP is a tool that helps control access to applications running on GCP based on identity and group membership.

Google Threat Intelligence

Google Threat Intelligence combines the unmatched depth of Google's Mandiant frontline expertise, the global reach of the VirusTotal community, and wide breadth of visibility, based on billions of signals across devices and emails. Google Threat Intelligence includes Gemini in Threat Intelligence, Google's AI-powered agent that provides conversational search across Google's vast repository of threat intelligence, enabling customers to gain insights and protect themselves from threats quickly

Google Security Operations SIEM

Google Security Operations SIEM enables enterprise security teams to detect, investigate, and respond to threats at speed and scale. Google Security Operations SIEM does this by collecting security telemetry data, aggregating it, normalizing it, and applying threat intelligence to identify the highest-priority threats.

Google Security Operations Security Orchestration, Automation and Response

Google Security Operations SOAR is a platform designed to help organizations detect, investigate, and respond to security threats in real time. The platform is powered by Google Cloud's infrastructure and leverages the ML capabilities of Google to automate and streamline security workflows.

Identity and Access Management

IAM enables the administration and authorization of access to specific resources and provides a unified view into security policies across entire organizations with built-in auditing.

Identity Platform

Identity Platform is a customer identity and access management (CIAM) platform delivered by Google Cloud enabling organizations to add identity management and user security to their applications or services.

Key Access Justifications

KAJ provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at rest to in use.

Managed Service for Microsoft AD

Managed Service for Microsoft AD is a Google Cloud service running Microsoft AD that enables customers to deploy, configure, and manage cloud-based AD-dependent workloads and applications. It is a fully managed service that is highly available, applies network firewall rules, and keeps AD servers updated with operating system patches.

Privileged Access Manager

Privileged Access Manager allows customers to control just-in-time temporary privilege elevation for select principals, and to view audit logs afterwards to find out who had access to what and when.

Organization Policy

Organization Policy provides customizable security guardrails to centrally enforce resource configuration compliance across resource hierarchies.

bernard@lotmaker.io

reCAPTCHA Enterprise

reCAPTCHA Enterprise helps detect fraudulent activity on websites using risk analysis techniques to distinguish between humans and bots.

Resource Manager API

Resource Manager API allows users to programmatically manage GCP container resources (such as Organizations and Projects) to group and hierarchically organize other GCP resources. This hierarchical organization enables users to manage common aspects of resources such as access control and configuration settings.

Risk Manager

Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including Center for Internet Security (CIS) Benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.

SecLM

SecLM, or, more specifically, the SecLM Platform (formerly known as Security AI Workbench or SAW), refers to the API and platform that Google has built based on the Sec-PaLM models. The platform orchestrates reasoning, extensions, retrieval augmented generation (RAG), and other techniques to leverage authoritative security data from sources, like Mandiant Advantage Threat Intelligence (MATI) and VirusTotal, and deliver the highest quality responses to security-related prompts.

Secret Manager

Secret Manager provides a secure method for storing API keys, passwords, certificates, and other sensitive data.

Security Command Center

Security Command Center is a log monitoring and security scanning tool that generates analytics and dashboards to help customers prevent, detect, and respond to Google Cloud security and data threats.

Sensitive Data Protection (including Cloud Data Loss Prevention)

Sensitive Data Protection is a fully managed service enabling customers to discover, classify, de-identify, and protect sensitive data, such as personally identifiable information.

VirusTotal

VirusTotal enables organizations to research and hunt for malware, to investigate security incidents, to automate analysis, and to keep user investigations private and secure.

VPC Service Controls

VPC Service Controls provides administrators with the ability to configure security perimeters around API-based cloud services (e.g., Cloud Storage, BigQuery, Bigtable) resources and limit access to authorized VPC networks.

Web Risk API

Web Risk API is a Google Cloud service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.

bernard@botmaker.io

Serverless Computing

Cloud Functions

Cloud Functions is a serverless compute solution that runs single-purpose functions in response to GCP events and HTTP calls (webhooks). Cloud Functions can be triggered asynchronously by Cloud Pub/Sub, Cloud Storage, GCP infrastructure events, and Firebase products. Cloud Functions scales automatically to meet request load, and the user does not need to manage servers or the runtime environment.

Cloud Functions for Firebase

Cloud Functions for Firebase consists of developer tools used for the development and deployment of Google Cloud Functions. Cloud Functions for Firebase enables developers to run their own back-end code that executes automatically based on HTTP requests and Firebase and GCP events. Developers' functions are stored in Google's cloud and run in a managed Node.js environment.

Cloud Run

Cloud Run (fully managed) is a serverless, managed compute platform that automatically scales stateless HTTP containers, running requests or event-driven stateless workloads. Cloud Run provides the flexibility to run services on a fully managed environment.

Cloud Scheduler

Cloud Scheduler is a fully managed, enterprise-grade cron job scheduler that allows customers to schedule jobs, including batch, big data jobs, and cloud infrastructure operations. It also acts as a single interface for managing automation tasks, including retries in case of failure, to reduce manual toil and intervention.

Cloud Tasks

Cloud Tasks is a fully managed service that allows customers to manage the execution, dispatch, and delivery of a large number of distributed tasks.

Datastream

Datastream is a serverless and easy-to-use change data capture (CDC) and replication service that allows users to synchronize data streams across heterogeneous databases and applications reliably and with minimal latency. Datastream supports streaming changes to data from Oracle and MySQL databases into Cloud Storage.

Eventarc

Eventarc is a fully managed service for eventing on GCP. Eventarc connects various Google Cloud services together, allowing source services (e.g., Cloud Storage) to emit events that are delivered to target services (e.g., Cloud Run or Cloud Functions).

Workflows

Workflows is a fully managed service for reliably executing sequences of operations across microservices, Google Cloud services, and HTTP-based APIs.

Storage

Backup for GKE

Backup for GKE enables data protection for workloads running in GKE clusters.

bernard@bitmaker.io

Cloud Filestore

Cloud Filestore is a service for fully managed Network File System (NFS) file servers for use with applications running on Compute Engine VM instances or GKE clusters.

Cloud Storage

Cloud Storage is GCP's unified object/blob storage. It is a RESTful service for storing and accessing data on GCP's infrastructure and combines the simplicity of a consistent API and latency across different storage classes with the reliability, scalability, performance, and security of GCP.

Cloud Storage for Firebase

Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for Firebase applications. Cloud Storage for Firebase is backed by Google Cloud Storage.

Parallelstore

Parallelstore is a parallel file system for high-performance computing and AI/ML workloads. Built on the Distributed Asynchronous Object Storage (DAOS) architecture, Parallelstore combines a fully distributed metadata and key-value architecture to deliver high-performance throughput and IOPS.

Persistent Disk

Persistent Disk provides a persistent virtual disk for use with Google Compute Engine and GKE compute instances. It is available in both SSD and hard disk drive (HDD) variations.

Other

Cloud Billing

Cloud Billing provides methods to programmatically manage billing for projects on GCP.

Google Earth Engine

Google Earth Engine combines a multi-petabyte catalog of satellite imagery and geospatial datasets with planetary-scale analysis capabilities. Scientists, researchers, and developers can use Google Earth Engine to detect changes, map trends, and quantify differences on the Earth's surface.

Google Cloud Marketplace

Google Cloud Marketplace offers ready-to-go development stacks, solutions, and services from third-party partners and Google to accelerate development. It enables the deployment of production-grade solutions, obtains direct access to partner support, and receives a single bill for both GCP and third-party services.

Google Cloud Skills Boost

Google Cloud Skills Boost is where you can access Google Cloud's entire catalog of labs and courses. Customer end users can discover learning paths, build in-demand cloud skills, track your activity progress, and validate your knowledge with badges.

Google Cloud VMware Engine

GCVE is a managed VMware-as-a-service that is specifically designed for running VMware workloads on Google Cloud Platform. GCVE enables customers to run VMware VMs natively in a dedicated, private, software-defined data center.

bernard@bolmaker.io

Tables

Tables is a lightweight, collaborative database to help organize and automate tasks or processes for small teams and businesses.

Data Centers

The above cloud products are serviced from Google data centers around the world. GCP offers global Cloud regions to provide customers with more hosting options, low cost, low latency, and application availability.

Google reinforces its commitment to data safety, privacy, and security by achieving certifications against rigorous global compliance standards, meeting the expectations of its third-party auditors, and ensuring that customer data remains secure and well-managed across all locations.

Google notifies stakeholders prior to updates and publishes information about specific services and activities across its various global locations at https://cloud.google.com/about/locations (as of the date of this report). The scope of this report does not include Google edge points of presence.

bernard@bothaker.io

Relevant Aspects of Internal Control

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

- *Control Environment*: Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- *Information and Communication*: Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control its operations.
- *Risk Assessment*: The entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed across the internal and external control environment, including third-party risk.
- *Monitoring Activities*: The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.
- *Control Activities*: Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's control objectives are effectively carried out.

This section briefly describes the four essential characteristics and other interrelated components of internal controls that support the achievement of the applicable C5 criteria as it pertains to the GCP products that may be relevant to customers into four broad areas:

- *Policies (Control Environment and Risk Assessment)*: The entity has defined and documented its policies relevant to the particular principle.
- *Communications (Information and Communication)*: The entity has communicated its defined policies to responsible parties and authorized users of the system.
- *Procedures (Control Activities)*: The entity placed in operation procedures to achieve objectives in accordance with its defined policies.

- *Monitoring (Monitoring Activities)*: The entity monitors the system and takes action to maintain compliance with its defined policies.

With respect to internal controls and relevant customers, Google defines “customers” as enterprise users that have entered into an agreement under which Google has agreed to provide GCP services as a data processor.

For the purposes of Google-Managed Multi-Cloud Services, customers select the Multi-Cloud Service Third-Party Providers on whose infrastructure the Google-Managed Multi-Cloud Service are deployed.

Google-Managed Multi-Cloud Services are defined in Google’s Service Specific Terms (https://cloud.google.com/terms/service-terms) (as of the date of this report) and are listed in the Google Cloud Platform Services Summary (https://cloud.google.com/terms/services) (as of the date of this report).

Policies

Internal Control Environment

Google has designed its internal control environment with the objective of providing reasonable, but not absolute, assurance as to the security, availability, confidentiality, and privacy of financial and user information, as well as the protection of assets from unauthorized use or disposition. Management has established and maintains an internal control structure that monitors compliance with established policies and procedures.

Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, confidentiality, and privacy controls.

To maintain internal compliance, Google has established a disciplinary process for noncompliance with the Code of Conduct, security and privacy policies, and other personnel requirements, which could include dismissal, lawsuits, and/or criminal prosecution.

The organization utilizes technologies to support the workforce in both remote and office work environments.

bernard@hotmaker.io

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Google Cloud Platform system. Commitments to customers are communicated via the Terms of Service, Google Cloud Platform System Service-Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations that the processors must meet to satisfy the organization’s obligations regarding the processing and security of customer data.

For Google-Managed Multi-Cloud Services, additional commitments to customers are communicated via the Google-Managed Multi-Cloud Services Data Processing and Security Terms Addendum.

System Requirements

Google has established internal policies and processes to support the delivery of Google Cloud Platform system products to customers. These internal policies are developed, in consideration of legal and regulatory obligations, to define Google’s organizational approach and system requirements.

The delivery of these services depends upon the appropriate internal functioning of system requirements defined by Google to meet customer commitments. The following processes and system requirements

function to meet Google's commitments to customers with respect to the terms governing the security and privacy of customer data:

- *Access Security*: Google maintains data access and logical security policies that are designed to prevent unauthorized persons and systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege.
- *Change Management*: Google requires standard change management procedures to be applied during the design, development, deployment, and maintenance of Google applications, systems, and services.
- *Incident Management*: Google monitors security event logs and alerts to determine the validity of security or privacy threats. Potential threats, including threats related to security and privacy, are escalated to the appropriate team, including incident management. Google's dedicated security personnel will promptly investigate and respond to potential and known incidents.
- *Data Management*: Google complies with any obligations applicable to it with respect to the processing of customer personal data. Google processes data in accordance with the GCP Terms of Service and/or Data Processing Agreements and/or Google-Managed Multi-Cloud Services Data Processing and Security Terms Addendum and complies with applicable regulations.
- *Data Security*: Google maintains data security and privacy policies and implements technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, or alteration, as well as unauthorized disclosure or access. Google takes appropriate steps to ensure compliance with the security measures by its employees, contractors, and vendors to the extent applicable to their scope of performance.
- *Third-Party Risk Management*: Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Google conducts routine inspections of subprocessors to ensure their continued compliance with the agreed upon security and privacy requirements. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from suppliers to comply with these practices.

bernard@bmaker.io

Internal Functions and Policies

Formal organizational structures exist and are available to Google personnel on the Company's intranet. The intranet provides drill-down functionality for identifying personnel in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas, including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Google has also developed the Data Security Policy, Data Classification Guidelines and Security Labels for Google Information, and privacy policies to establish procedures for information labeling and handling in accordance with the Google guidelines. Additionally, Google maintains policies that define the requirements for the use of cryptography, as well as policies for securing mobile devices to help ensure Company and customer data are protected. Policies are reviewed annually, and other materials derived from policies, such as guidelines, FAQs, and other related documents, are reviewed and updated as needed.

Communications

Information and Communication

To help align its business strategies and goals with operating performance and controls, Google has implemented various methods of communication to ensure that all interested parties and personnel understand their roles and responsibilities and that significant events are communicated in a timely manner. These methods include:

- Orientation and training programs for newly hired employees
- An information security and privacy training program that is required to be completed by relevant personnel annually
- Requirements for employees of the organization to acknowledge the Code of Conduct
- Regular management meetings for updates on business performance and other business matters
- Management development and communication of Company goals and responsibilities on a periodic basis with amendment as needed, as well as the evaluation and communication of results to employees
- Detailed job descriptions; product information (including system and its boundaries); and Google's security, availability, confidentiality, and privacy obligations that are made available to employees in the intranet
- The use of email messages to communicate time-sensitive messages and information
- Publishing security and privacy policies and security-related updates on its intranet, which is accessible by all Google employees, temporary workers, contractors, and vendors

Google has communicated to employees and the extended workforce instructions and mechanisms for reporting potential security and privacy concerns or incidents. Google has also implemented various methods of communication to help ensure that user entities understand Google's commitments to security, availability, confidentiality, and privacy for GCP and to help ensure that significant events are communicated to user entities in a timely manner.

The primary conduit for communication is the Google website, which is made available to all user entities. The website includes blog postings on the official Google blog (as of the date of this report) and various product-specific blogs support forums and release notes. Google provides 24x7 assistance, including online and phone support, to address customers' concerns. Customer service and/or technical support representatives are also an important communication channel, as they maintain records of problems reported by the user entity. Customer service representatives also assist in communicating information regarding new issues and/or developments, changes in services, and other information. Additionally, Google maintains an established Board of Directors that operates independently from management. The Board exercises oversight over management decisions.

For Google-Managed Multi-Cloud Services, responsibilities of Multi-Cloud Service Third-Party Providers are defined in the Enterprise Agreement signed between them and Google. Multi-Cloud Service Third-Party Providers only process data as instructed by Google, which acts on behalf of its customers. The Multi-Cloud Service Third-Party Providers' Enterprise Agreements, AWS Service Terms, and Data Processing Terms define Google's data subject rights.

As a data processor, Google limits processing to what is specified in the contracts with the controller or as otherwise required under applicable data protection laws. Customer data is processed in accordance with

bernard@potmeker.nl

the Cloud Data Processing Addendum, which is externally published at https://cloud.google.com/terms/data-processing-addendum (as of the date of this report). As data controllers, customers are responsible for communicating choices available to users regarding collection, use, retention, disclosure, and disposal of personal information. Google does provide customers with mechanisms to access, modify, delete, and export customer data.

Procedures

Hiring Practices

Google has designed formal global hiring practices to help ensure that new and transferred employees are qualified for their functional responsibility. Every employee has a written job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Google. Where local labor law or statutory regulations permit, Google may conduct criminal, credit, and/or security checks on all potential employees, temporary workers, and independent contractors, as well as verification of the individual's education, previous employment, and referrals. The specifics or extent of background checks performed depend on the position and location for which the individual is applying.

Upon acceptance of employment, all employees, including extended workforce personnel, are required to execute a confidentiality agreement and acknowledge receipt of and compliance with Google's Code of Conduct. The confidentiality and privacy of customer data is emphasized in Google's employee handbook and also during new employee orientation. It is the responsibility of every employee to communicate in a timely manner significant issues and exceptions to an appropriate higher level of authority within the Company.

Risk Management

Risk management is a pervasive component of GCP provided by Google to user entities, irrespective of the location or business area. The Google teams that lead engineering, sales, customer service, finance, and operations have the primary responsibility to understand and manage the risks associated with their activities for user entities using GCP products. These risk management and mitigation activities are critical and have been integrated into Google's repeatable process models.

At a corporate level, there are multiple functional areas, including Legal; Information Security; Internal Audit; Privacy Engineering; Privacy Compliance; Alphabet Regulatory Response Investigations and Strategy (ARRIS); Privacy, Safety and Security (PSS); the Cloud Chief Information Security Officer (CISO); and the Office of Compliance and Integrity (OCI), which provide risk management support through policy guidelines and internal consulting services.

Google develops and maintains a risk management framework to manage risk to an acceptable level for GCP. Google has developed vulnerability management guidelines and regularly analyzes the vulnerabilities associated with the system environment. Google takes into consideration various threat sources, such as insider attacks, external attacks, errors and omissions, and third-party-related issues such as inadvertent disclosure of Google confidential information (e.g., payroll data) by a third party.

Factors, including threat-source motivation and capability, the nature of the vulnerability, and the existence and effectiveness of current controls, are considered in determining the probability that a potential vulnerability may be exposed. The likelihood that a potential vulnerability could be exposed by a given threat-source is designated by Google as either high, medium, or low.

bernard@bormaker.io

Google then determines the potential adverse impact resulting from a successful exploitation of vulnerabilities. The highest priority is given to any potential compromise of user data.

The level of risk and remediation priority for a particular threat/vulnerability pair is expressed as a function of:

- The likelihood of a given threat source's attempt to exploit a given vulnerability
- The impact should a threat source successfully expose the vulnerability
- The effectiveness of existing security and privacy controls for mitigating risk

Google performs a formal risk assessment for each of its in-scope product areas assessment at least annually and determines the likelihood and impact of identified risks, using qualitative and quantitative methods. The likelihood and impact associated with each risk is determined independently, considering each risk category. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management. Management also proactively identifies emerging risks for product areas to include within their respective risk assessments.

Google has an established Internal Audit function and compliance specialists responsible for evaluating the effectiveness of controls in addressing a given risk, including, among other controls, identity management, source code management, and authentication infrastructure controls, against requirements. They perform risk-based assessments and issue audit reports regarding their analysis. Remediation of security and privacy deficiencies is tracked through internal tools and remediation plans.

Third-Party Risk Management

Google may utilize third-party vendors to support GCP. Prior to onboarding, Google completes a nondisclosure agreement and then performs vendor security assessments (VSAs) on all vendors with whom Google shares confidential or sensitive information, including user data. A VSA is an important health check of a vendor's operational security posture. It assesses whether a vendor adheres to generally accepted security and data protection best practices. The outcome of a VSA is a risk assessment and a determination of whether a vendor should or can be used (approval). Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted. At a high level, each of these assessments involves:

- An initial risk assessment to determine if a VSA is required (i.e., instances where vendors handle, collect, or access any user data or business data that is classified as need-to-know)
- A risk-based review of the policies, processes, and controls the vendor has in place compared to generally accepted security best practices using questionnaire-based information gathering
- A tailored risk assessment for Mergers and Acquisitions due diligence or third-party risk management in partnerships, joint ventures, and other complex relationships
- Reviewing and citing independent verification of the security state of systems relevant to Google's use of the vendor

A subset of vendors is considered to be subprocessors based on the data sharing relationship between the vendor and Google. Google utilizes subprocessors to support GCP and has established expectations for subprocessors related primarily to security and privacy. The meeting of these expectations is subject to periodic business review by Google. However, subprocessors do not manage or perform any of the GCP controls tested herein.

bernardo@bothbyer.ro

Google maintains a Subprocessor Audit Program that is tasked with the periodic information security and privacy assessment of subprocessors using ISO 27001 as the baseline. Google evaluates conformance to these expectations through inspection of third-party ISO certifications, SOC 2 reports, or on-site or virtual inspections. In such cases where Google identifies any deviations in the performance of subprocessor controls, findings are evaluated by Google and discussed with the subprocessors upon completion of the audit. When applicable, remediation plans are put in place to resolve issues in a timely manner.

Google has also implemented a Subprocessor Data Processing Agreement (SDPA) to contract with subprocessors. The SDPA defines the security and privacy obligations that the subprocessor must meet to satisfy Google's obligations regarding customer data, prior to Google granting such access. Per the Data Processing Addendum, Google notifies the customer prior to onboarding a new subprocessor. Information about the subprocessor, including function and location, is externally published at https://cloud.google.com/terms/subprocessors (as of the date of this report).

Enterprise agreements are signed between Google and the Multi-Cloud Service Third-Party Providers, which outline the expectations for subprocessors related primarily to security and privacy through Service Terms. Information about Multi-Cloud Service Third-Party Providers and their locations is published (see https://cloud.google.com/terms/mcs-providers) (as of the date of this report).

bernardo@botmaker.io

Data Confidentiality and Privacy

Google has established training programs for privacy and information security to support data confidentiality and privacy. Relevant personnel are required to complete these training programs annually.

All new product and product-feature launches that include collection, processing, or sharing of user data are required to go through an internal security and privacy design review process. These reviews are performed by the Security, Legal, and Privacy teams. Databases and websites exist to track and monitor progress of GCP project developments. In addition to the preventative controls, Google has also established detective measures to investigate and determine the validity of security threats. In the case of an incident, there are incident response processes to report and handle events related to topics such as security and confidentiality. Google establishes confidential agreements, including nondisclosure agreements, for preserving the confidentiality of information and software exchange with external parties.

For government agency data requests, Google has mechanisms in place to record and track transfers and disclosures of user's data to third parties. Customers are notified of third-party data requests in accordance with any procedure and time period agreed in the contract unless such disclosure is prohibited by law. As a data processor, Google limits disclosures of customer data to disclosures that are legally required or authorized by the data controller.

Information Security Program

Google's information security program is designed to safeguard information assets against unauthorized use, disclosure, modification, damage, or loss. The program includes educating Google personnel about security-related issues, assessing current policies and developing new policies, assisting in strengthening technical measures to protect corporate resources, and developing mechanisms to react to incidents and events that could affect Google's information assets.

Google has dedicated security teams responsible for educating Google personnel about security and assisting product teams with security design. Information security is managed by a dedicated Security and Privacy executive who is independent of Information Technology management responsibilities and may escalate security issues or concerns directly to the Board. The Security team also reviews the security

practices of vendors and the security posture of vendor products for all vendors with whom Google shares confidential or sensitive information.

Google has security policies that have been reviewed and approved by management and are published and communicated to employees and vendors with access to the Google environment. Google's security policies describe security objectives, provide a security framework, and emphasize the importance of security to Google's business. Security policies are reviewed at least annually. Policies, FAQs, and guidelines are updated as needed.

For Google-Managed Multi-Cloud Services, the Google-Managed Multi-Cloud Services Data Processing and Security Terms Addendum outlines the additional role and responsibilities between Google and Multi-Cloud Service Third-Party Providers. Google enters into data processing agreements with the Multi-Cloud Service Third-Party Providers that impose the data protection obligations described in Article 28(3) of the EU's General Data Protection Regulation (GDPR) on the Multi-Cloud Service Third-Party Providers for its processing of any personal data within the Google-Managed Multi-Cloud Services.

Information Privacy Program

Google's Information Privacy program is designed to safeguard information assets against unauthorized use, access, disclosure, modification, damage, or loss, as well as the privacy of customer data. The program includes, but is not limited to, developing and managing privacy policies; developing privacy requirements for products and services, including reviewing data usage to ensure processing of customer data is in accordance with the applicable data protection agreements entered into between Google and customers based on applicable data protection laws and regulations; and developing mechanisms to react to privacy incidents and events that could affect Google's information assets and customer data. Google has dedicated privacy teams responsible for educating Google personnel about privacy, assisting product teams with privacy design, and overseeing privacy practices at the Company. Google has privacy policies that have been reviewed and approved by management and are published and communicated to employees and vendors with access to the Google environment. Google's privacy policies describe privacy objectives, provide a privacy framework and required practices, and emphasize the importance of privacy to Google's business. Privacy policies are reviewed at least annually. Policies, FAQs, and guidelines are updated as needed.

Google's role as a data processor and the scope of the processing are defined in the applicable Data Processing Addendum, which is externally published at https://cloud.google.com/terms/data-processing-addendum (as of the date of this report).

Network Architecture and Management

The GCP system architecture utilizes a fully redundant network infrastructure. Border routers that provide the connection point between GCP and any Internet service providers are designed to run in a redundant configuration. Where border routers are in use, firewalls are also implemented to operate in a redundant configuration.

Google has implemented perimeter devices to protect the Google network from external attacks. Google segregates networks based on service, user, and information system type. The network is managed via specialized tools. Google employs automated tools to inventory network devices and machines. Authorized security and network engineers access the network devices (production routers and switches) to monitor, maintain, manage, and secure the network through these tools.

bernard@bountiker.io

Network monitoring mechanisms are in place to detect and disconnect access to the Google network from unauthorized devices. Configurations of perimeter devices are centrally managed. Current and previous versions of each router configuration are maintained. Google has documented procedures and checklists for configuring and installing new servers, routers, and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet.

Google has a firewall configuration policy that defines acceptable ports that may be used on a Google firewall. Only authorized services and protocols that meet Google's requirements are permitted access to the network. The firewalls are designed to automatically deny all unauthorized packets not configured as acceptable. Administrative access to the firewalls is limited to authorized administrative personnel using the SSH protocol and two-factor authentication. Changes to network configurations are peer-reviewed and approved prior to deployment. Google has implemented automated controls on network devices to identify DDoS attacks. Google has established incident response processes to report and handle such events (see the Incident Management section).

For Google-Managed Multi-Cloud Services, Google utilizes VPC capabilities provided by the Multi-Cloud Service Third-Party Providers to configure network infrastructure and segregate networks based on the types of services, users, and information systems. Cloud firewalls protect the Google-managed network from external attacks and limit access to only authorized services and connections originating from the Google network based on the configurations and rules managed by Google.

Authentication, Authorization, and Administration

Strong authentication and access controls are implemented to restrict access to GCP production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google uses encryption to secure user data in transit between Google production facilities. Access to internal support tools, those used by Google operational staff to maintain and troubleshoot the systems for GCP, is controlled via access control lists (ACLs), thus limiting the use of these tools to only those individuals who have been specifically authorized.

Digital certificates used for machine authentication and data encryption are issued by an internal Google certificate authority. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to the Google corporate machines requires a Google-issued digital certificate installed on the connecting device and two-factor authentication.

Google follows a formal process to grant or revoke employee access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system that utilizes SSH and TLS certificates help provide secure and flexible access. These mechanisms are designed to grant access rights to systems and data only to authorized users. Additionally, access requests via "on-demand request" mechanisms are reviewed and approved by a second individual prior to being granted, and the event is logged.

Both user and internal access to customer data are restricted through the use of unique user account IDs and via the Google Accounts Bring Your Own Identity (BYOID) system externally. Access to sensitive systems and applications requires two-factor authentication in the form of unique user IDs, strong passwords, security keys, and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data (and other need-to-know data) is appropriate and authorized. Access to

bernardo@bothunter.io

production machines, network devices, and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. Critical access groups are reviewed semiannually under the direction of the group administrators to ensure that access has been removed for employees who no longer have a business need for such access.

Access authorization in GCP is enforced at all relevant layers of the system. The granting or modification of access rights is based on the user's job responsibilities or on a need-to-know basis and must be authorized and approved by the user's functional manager or system owners. Approvals are managed by workflow tools and logged. Production system access is granted only to individuals who have completed the required security and privacy training and require this level of access to perform required tasks. Access to individual production systems via critical access groups is reviewed periodically by the system owners, and inappropriate access is removed for Google personnel who no longer have a business need for such access. Access to all corporate and production resources is automatically removed upon submission of a termination request by the manager of any departing employee, or by the appropriate Human Resources manager.

For Google-Managed Multi-Cloud Services, Google utilizes identity and access management capabilities provided by the Multi-Cloud Service Third-Party Providers to restrict access to Google-managed infrastructure via ACLs. Google-managed infrastructure can only be accessed from Google-owned machines, and Google accounts are used to access environments deployed on Multi-Cloud Service Third-Party Providers infrastructure. Access requires two-factor authentication in the form of unique user IDs, strong passwords, security keys, and/or certificates. In addition, every time access is requested, a temporary token is generated via access "on demand request" mechanisms to access the environments on Multi-Cloud Service Third-Party Providers infrastructure. The access is managed via the Google access group management system using dedicated groups associated with environments deployed on Multi-Cloud Service Third-Party Providers' infrastructure. Encryption provided by the Multi-Cloud Service Third-Party Providers is used to protect user authentication and to administrator sessions transmitted over the Internet; all sessions between the Google network and the Google-managed network in the Multi-Cloud Service Third-Party Providers environments are encrypted.

bernard@hormer.io

Password Guidelines

Google personnel are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection, and management guidelines, which enforce the following:

- Minimum length
- Complexity
- History
- Idle time lockout setting

Password configuration requirements are enforced by internal systems. In addition to the security requirements enforced during configuration, internal passwords are subject to cryptographic hashing to mitigate the risk of unauthorized disclosure or modification.

Google has supplemented passwords with a two-factor authentication requirement for internal personnel to access sensitive internal corporate and production services and to access GCP in the production environment from the corporate network. Two-factor authentication provides additional protection to prevent user account manipulation in case the user's password is compromised.

GCP end users can also authenticate in one of three ways:

- Using their user ID and a password that is managed by Google
- Using a two-step authentication process that includes their user ID, password, and a security key
- Through the Security Assertion Markup Language (SAML)-based single sign-on (SSO) process, which uses the user entity's own account management system to authenticate users, and a certificate with an embedded public key, which is registered with Google for each customer entity

For Google-Managed Multi-Cloud Services, Google accounts are used to access environments deployed on Multi-Cloud Service Third-Party Providers' infrastructure; therefore, the same password guidelines apply. Multi-Cloud Service Third-Party Providers' password policies apply to the accounts, which were created for Google by providers when the environment was initially created.

Physical Access – Data Center Physical Security

Google maintains consistent policies and standards across its data centers (both Google-owned and third-party-owned) for physical security to help protect production servers, network devices, and network connections within Google data centers. Guidelines for evaluating the security of data centers are described in Google's data center security evaluation criteria. Additionally, data center personnel perform periodic surveys and reviews of data centers. Data centers that house GCP systems and infrastructure components are reviewed at least annually for ongoing security compliance. A security report is then created summarizing any observations, deviations, or action items. This report is presented to executive management for review and approval. Corrective actions are taken when necessary. Google also generates a quarterly report of data center badge access, which is reviewed and approved by data center operations management. Inappropriate access is removed in a timely manner. The data center security evaluation criteria elements include:

- Security guards, access badges, and video cameras are in use.
- Entrances, cages, suites, and rooms in use by Google are secured by badge readers, secondary identification mechanisms, and/or physical locks.
- Emergency exit points from server rooms are alarmed.
- Video cameras exist to monitor the interior and exterior of the facility.
- On-site security personnel are present 24x7.

Formal access procedures exist for allowing physical access to the data centers. There are documented procedures for issuing badges to staff and visitors, and the owner of each badge is tracked and documented. All entrants to the data center, whether they are Google employees, visitors, or contractors, must identify themselves and show proof of identity to Security Operations.

Valid proof of identity consists of a photo ID issued by (i) Google or (ii) a governmental entity. Only validated visitors and authorized Google employees and contractors are permitted to enter the data centers. Authorized Google Data Center Approvers must approve all visitors in advance for the specific data center and internal areas to be visited.

After the individual's access authorization is verified, the visit is logged, and access is granted for the specified dates and times. These logs are retained by Google security for review as needed. Visitors are provided a temporary badge and must be escorted by an authorized Google employee to access areas beyond the lobby. When the visitors leave the data center, they must return the visitor badge.

bernard@cloudmarket.ie

Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas. Google authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items. Google also utilizes automated mechanisms to track inventory of all production machines and inventory of all serialized server components. Only authorized Google employees or contractors permanently working at the data centers are permitted to request standing access to the facility areas needed for their role and responsibilities. Data center access requests must be made through internal tools and require the approval of authorized data center personnel. All other Google employees and authorized contractors requiring temporary data center access must also have an approved access request and register at the guard station upon arrival. User access lists to data center server areas are reviewed quarterly, and inappropriate access is removed in a timely manner.

Data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network infrastructure are connected to redundant power sources that are physically protected from disruption and damage in addition to emergency power, which is available in the event of a loss of power. Google performs preventative and regular maintenance on fire detection and protection equipment, uninterruptible power supply (UPS), generators, HVAC, and emergency lighting systems. Please refer to the Data Centers section above for a list of Google's data center locations.

For Google-Managed Multi-Cloud Services, Google relies on Multi-Cloud Service Third-Party Providers for physical security as the physical locations are controlled by providers. Google conducts a periodic assessment of the Multi-Cloud Service Third-Party Providers control environment via review of their SOC 2 reports. Google reviews that complementary user entity controls (CUECs) are implemented by Google as instructed by the Multi-Cloud Service Third-Party Providers, and no deficiencies pose risk to Google customers.

bernard@bonnaker.ru

Change Management

Changes to GCP are delivered as software releases through three pipelines:

- Product functionality changes or builds related to the service running in Google's production environment
- Images, downloads, or software updates made available to customers
- Open-source code packages maintained in a public source code repository

Changes, including configuration changes, code modifications, and new code creation, follow this change management process. Change management policies and guidelines, including code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented. Each service has documented release processes that specify the procedures to be used, including definition of the scope of changes to be delivered, source code control, code review, building, testing, and record keeping. Development, testing, and build environments are separated from the production environment.

The change process starts with a developer checking out a copy of the head source code files from the source code management system to modify them. Once development is complete, the developer initiates applicable testing and code reviews. Once the change has received the appropriate code review, the changes can be submitted, making it the new head version. Google requires that production code reviewers be independent of the developer assigned to the change and follow Google coding standards, in accordance with their policy. Production code reviews are systematically enforced. Emergency changes are reviewed and approved weekly by corresponding product owners.

Once the code is merged, it can be used to build software binaries. During the build process, code is subject to automated testing, the results of which are monitored by engineers. Successfully built binaries can be migrated to staging or quality assurance (QA) environments, where they can be subject to additional review. When software is ready for deployment to production, it is deployed in a controlled manner with monitoring in place to notify engineers of anomalies in the deployment. The process from build to release is aided by several tools that automate tasks, including testing and deployment. Employees at Google have the ability to view changes; however, access to modify code and approve changes is controlled via functionality of internal tools that support the build and release process. Changes to customer-facing services that may affect confidentiality, processing integrity, and/or availability are communicated to relevant personnel and impacted customers.

Guidelines are made available internally to govern the installation of software on Company-owned assets. Additionally, tools are utilized to detect any deviation from pre-defined operating system configurations on production machines and to correct it automatically. This allows for an easy rollout of updates to system files in a consistent manner and helps ensure that machines remain in a known current state.

For Google-Managed Multi-Cloud Services, Google standard systems and tools are used to manage changes and deploy releases. A workflow management system is used to deploy build binaries to Google-managed environments hosted on Multi-Cloud Service Third-Party Providers' infrastructure.

Emergency changes to production environments are considered to be a "break-glass" scenario. Such changes have to be deployed by accessing the Google-managed environments hosted on Multi-Cloud Service Third-Party Providers' infrastructure with administrative permissions. Break-glass access requires multi-party authorization from the product management team, which includes justification for access. Changes made via an emergency procedure must also be made via the standard process as well; otherwise, emergency changes will be overridden by the next automated deployment.

Change management automation monitors any changes to the production environments, and will attempt to restore its state to the intent in Google source code. If an attempt fails, alerts are raised, and on-call teams are notified to investigate and remediate the change.

Google-managed environments hosted on Multi-Cloud Service Third-Party Providers' infrastructure are periodically fully rebuilt from the Google source code, which enables scaling of the services and maintains the pre-defined operating system configurations.

bernard@bdmaker.in

Vulnerability Management

The goal of Google's vulnerability management program is to investigate and respond to all relevant security vulnerabilities. The Vulnerability Management Guidelines describe how vulnerabilities are detected, classified, and remediated at Google. As part of this program, the Security Operations team conducts network vulnerability scans to detect vulnerabilities in software, systems, and network devices. These scans are conducted continuously to identify and remediate potential vulnerabilities.

External third-party penetration tests are performed at least annually on Google systems and networks. The scope and frequency of testing is determined by the Google Security and Cloud Compliance teams and is based on their understanding of the Company's current risk environment, as well as its current regulatory and compliance requirements. Google also conducts six monthly network segmentation tests and logical separation of multi-tenant data to identify vulnerabilities that could lead to critical infrastructure service interruption, destruction of facilities, or compromise of sensitive systems and data.

For Google-Managed Multi-Cloud Services, Google deploys scanning tools in Google-managed environments hosted on Multi-Cloud Service Third-Party Provider infrastructure. Scans are conducted on

an ongoing basis. Further, results are sent to Google daily and are incorporated into Google's vulnerability management program.

Incident Management

Dedicated on-call personnel and Security and Privacy Incident Response teams are responsible for managing, responding to, and tracking incidents. These teams are organized into formalized shifts and are responsible for helping resolve emergencies 24x7. Incident response policies are in place and procedures for handling incidents are documented.

For Google-Managed Multi-Cloud Services, Google involves Multi-Cloud Service Third-Party Providers as needed. Google has full control over Google-managed environments on Multi-Cloud Service Third-Party Providers' infrastructure, and, therefore, is able to independently manage incidents. Any incidents with Multi-Cloud Service Third-Party Providers' backend infrastructure are handled by Multi-Cloud Service Third-Party Providers, involving Google as a customer when needed.

Incident Alert and Recording

Log sources are used to generate alerts whenever an anomaly occurs. Production monitoring tools, in response to an anomaly, automatically generate alerts to relevant teams based on the anomaly configurations set by each team. An anomaly may also be manually documented by a Google employee when an issue is identified or in response to a customer service request.

Production systems are configured to send system events to monitoring and alerting tools. Google personnel use these tools to respond to potential incidents, including security and privacy incidents.

Alerts capture the information necessary for initial response, including origin, service description, and impacted area. Alerts are addressed by relevant teams to identify if the anomaly indicates an issue or potential issue. If necessary, incidents are created for alerts that require additional investigation. Additional details can be added to the incident to supplement the initial alert(s). The incident is assigned an initial severity level to prioritize mitigation efforts to incidents of greatest impact. Each severity level has been formally defined to capture the importance of each incident or problem type. There are established roles and responsibilities for personnel tasked with incident management, including the identification, assignment, managed remediation, and communication of incidents.

Incident Escalation

Google has documented escalation procedures and communication protocols that address the handling of incidents and the notification of appropriate individuals. Escalated issues are treated with higher urgency and are often shared with a wider audience.

Alert escalation is facilitated by either an internal escalation tool or manual escalation based on Google-wide and team-specific escalation criteria. Production monitoring tools are integrated with the alert manager tool and communicate with the escalation tool via email and notification to on-call staff via pager. The escalation time and contacts are defined in the escalation tool configuration files. If the tool does not receive an acknowledgement from the notified contacts, this leads to automated escalation.

Incident Resolution

After gathering the necessary information about the incident, the incident ticket is assigned to the appropriate support area based on the nature of the problem and/or the root cause. Incidents are usually forwarded to one of the corresponding technical departments:

- System Reliability Engineers/Software Engineers

bernard@bitmaker.io

- Networks
- Database Administration
- System Administration
- Application Administration
- Facilities
- Network Security
- Platform Support
- Legal

The incident ticket is closed upon resolution of the incident. Google also has an established postmortem process for performing technical analysis of incidents after the fact to identify root cause issues, document lessons learned and implement fixes to prevent future incidents. Processes for notifying customers of data security and privacy incidents that affect their accounts in accordance with disclosure laws or contractual agreements are established and implemented.

Data Retention and Deletion

Google has procedures in place to dispose of confidential and need-to-know information according to the Google data retention and deletion policy. Additionally, Google maintains defined terms regarding the return, transfer, and disposal of user data and makes these terms available to customers.

For Google-Managed Multi-Cloud Services, the responsibilities of Multi-Cloud Service Third-Party Providers regarding data retention and deletion are defined in the Enterprise Agreements signed between the providers and Google. Google is responsible for managing the data processed in Google-managed environments on Multi-Cloud Service Third-Party Providers' infrastructure. Customer data is only processed and not stored in Google-managed environments.

Storage Media Security

Integrity checks are in place at the application level and file system level to ensure data integrity. At the application level, checksum comparison is performed to protect against upload corruptions. File system consistency checks are also deployed at the storage layer using user-level programs that verify the integrity of the data. At the machine level, an integrity check system is used to synchronize system files on the root partition of production machines with a standard base image.

Google utilizes barcodes and asset tags to track the status and location of data center equipment from acquisition to installation, retirement, and destruction. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies such as full disk encryption (FDE) and drive locking to protect data at rest. Personally identifiable information on removable media leaving Google facilities must be approved and encrypted.

When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi-stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

leonard@notmaker.no

For Google-Managed Multi-Cloud Services, Google relies on Multi-Cloud Service Third-Party Providers for physical security, including storage media security, as the physical locations are controlled by providers. Google conducts a periodic assessment of the Multi-Cloud Service Third-Party Providers' control environments via review of their SOC 2 reports. Google reviews that CUECs are implemented by Google as instructed by the Multi-Cloud Service Third-Party Provider and that no deficiencies pose risk to Google customers.

Redundant Architecture

GCP runs in a multi-tenant, geographically distributed environment on synchronized, internal system atomic clocks and global positioning systems (GPSs) to support the availability of services through the use of redundant architecture. Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed among a shared infrastructure. For GCP, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Structured data is then stored in large, distributed databases built on top of this file system.

The data centers are connected through multiple encrypted network links and interfaces, providing high availability by dynamically load balancing across those sites. Google uses a dashboard that provides details such as resource footprint, CPU capacity, and random-access memory availability to monitor resource availability across its data centers and to validate that data has been replicated to more than one location.

For Google-Managed Multi-Cloud Services, Google relies on Multi-Cloud Service Third-Party Providers' redundancy since the backend infrastructure is managed by the providers. Google configures environments hosted on Multi-Cloud Service Third-Party Providers' infrastructure to enable service-level redundancy for its customers.

Disaster Recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, Google designs its infrastructure and services to be resilient to failures of software, hardware, or facilities. Redundant architecture and resources are distributed across at least two geographically dispersed data centers to support the availability of services. Network connections between the data centers help ensure swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage and system administration.

Google's disaster recovery program enables continuous and automated disaster readiness, response, and recovery of Google's business, systems, and data. Google conducts disaster resiliency testing at least annually to provide a coordinated venue for infrastructure and application teams to test communication plans, failover scenarios, operational transition, and other emergency responses. Disaster resiliency testing covers reliability, survivability, and recovery. Teams that participate in the disaster resiliency exercise develop testing plans and postmortems that document the results and lessons learned from the tests.

Additionally, business continuity plans defining how personnel should respond to disruptions are maintained and made available internally and maintained. Disaster resiliency testing, which covers reliability, survivability, and recovery, is also conducted on an ongoing basis, and at least annually.

Monitoring

Functional areas across the organization are accountable for designing, implementing, and operating controls to reduce risk across the organization and to engage with management for assessing controls. Management performs periodic assessments of the control environment for specific areas, such as identity

bernard@botmaker.io

management, source code management, and authentication infrastructure controls. Google plans and coordinates system security-related and privacy-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users. Independent Internal Audit teams also perform regular audits over these areas of the control environment, and the reports associated with the audits are made available to the audit committee and stakeholders. In addition, monitoring activities have been described below to communicate how monitoring is performed for GCP.

Security Monitoring

Google has implemented monitoring tools to detect and report security events. Antivirus, phishing detection, and antimalware/antispam tools are also in place to protect Google's information assets. Google also maintains security event logs for privileged access, access to user data, authorized access attempts, and unauthorized access attempts. Logical access to security event logs is restricted to authorized personnel. Security event logs are monitored continuously using a Google proprietary security event management (SEM) system to detect intrusion attempts and other security-related events. The SEM is supplemented with codified logic, which creates the "hunts" that trigger automated alerts to security personnel. The security alerts are generated for further investigation (manual and automated hunts) based on predefined thresholds. When a vulnerability has been identified, the Security team determines the appropriate response and tracks the issue through to resolution. The owners of the affected component(s) determine the appropriate response based on the severity and defined response criteria of the vulnerability.

For Google-Managed Multi-Cloud Services, Google involves Multi-Cloud Service Third-Party Providers as needed. Google has full control over Google-managed environments on Multi-Cloud Service Third-Party Providers' infrastructure and, therefore, is able to independently manage alerts and incidents, as well as monitor the environment under Google's responsibility. Any incidents with Multi-Cloud Service Third-Party Providers backend infrastructure are handled by Multi-Cloud Service Third-Party Providers, involving Google as a customer when needed.

Availability Monitoring

Resource management procedures are also established to monitor, maintain, and evaluate capacity demand. Google uses a dashboard that provides details such as resource footprint, CPU capacity, and random-access memory availability to monitor resource availability across its data centers and to validate that data has been replicated to more than one location.

In order to maintain sufficient capacity in Google-managed environments hosted by Multi-Cloud Service Third-Party Providers, Google reserves the resources needed based on the forecast, including required redundancy. Google monitors the utilization of reserved resources and manages the quota appropriately based on the monitoring alerts.

Confidentiality Monitoring

Google has established incident response processes to report and handle events related to confidentiality as described under Incident Management above.

Privacy Monitoring

As described above, Google restricts and monitors access to customer data to only those with a valid business purpose and further restricts the processing of customer data to authorized individuals. Google has an incident monitoring and response program designed to alert and take action if unauthorized access

bernard@hotmaker.fr

is discovered. New products and services are reviewed prior to launch to ensure customer data use is in accordance with the Data Processing Addendum.

Complementary User Entity Controls (CUECs)

GCP is designed with the assumption that user entities (also referred to as customers) implement certain policies, procedures, and controls. In certain situations, the application of specific or additional controls by the user entity may be necessary to achieve the applicable criteria stated in the description. Therefore, each user's controls must be evaluated in conjunction with the controls summarized in Section 3 and Section 4 of this report.

This section describes those additional policies, procedures, and controls that Google recommends user entities consider implementing to complement Google's policies, procedures, and controls. Management of the user entity and the user entity's auditor should consider whether the following controls have been placed in operation at the user entity:

- Organization and Administration
  - Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of GCP.
  - Customers are responsible for establishing organizational policies and procedures for the use or integration of third-party services.
  - Customers are responsible for reviewing the information security policies and the security capabilities in GCP to determine their applicability and modify their internal controls as appropriate.
  - Customers are responsible for providing the appropriate training to end users on proper use of GCP consistent with the Acceptable Use Policies and Terms of Service. Acceptable Use Policies are available at (or such URL as Google may provide):
    - GCP: https://cloud.google.com/terms/aup (as of the date of this report).
    - SecOps Services Agreement: https://cloud.google.com/terms/secops (as of the date of this report).
  - Customers are responsible for ensuring that end users are trained on the organizational policies and procedures relevant to the use of GCP.
  - Customers are responsible for defining, documenting, and making available to users the procedures for the operation of their instance of GCP.
  - Customers are responsible for identifying and managing the inventory of information assets on GCP.
  - For Google-Managed Multi-Cloud Services, customers are responsible for having a separate agreement in place with their selected Multi-Cloud Service Third-Party Provider that governs the Multi-Cloud Service Third-Party Provider's processing of customer data on behalf of customer ("Multi-Cloud Service Data Processing Terms").
  - For Google-Managed Multi-Cloud Services, customers are responsible for administering the connection between Google Cloud Platform resources and customer's resources hosted by the Multi-Cloud Service Third-Party Providers.
  - For Google-Managed Multi-Cloud Services, customers are responsible for restricting data location in accordance with C5 certified regions of their selected Multi-Cloud Service Third-Party Provider.

bernard@bormaker.io

- Logical Access
  - Customers are responsible for defining and maintaining policies and procedures governing the customer's administration of access to GCP.
  - Customers are responsible for provisioning service availability, user roles, and sharing permissions within GCP consistent with customer organizational policies.
  - Customers are responsible for implementing secure login procedures to access GCP consistent with customer access management policies.
  - Customers are responsible for provisioning, maintaining, and disabling users' access in accordance with customer access management policies.
  - Customers are responsible for reviewing users' access rights periodically, consistent with customer organizational policies, to mitigate the risk of inappropriate access.
  - Customers are responsible for enabling and enforcing the use of two-factor verification on privileged administrator accounts.
  - Customers are responsible for establishing procedures to allocate the initial password to access GCP to end users when Google password authentication is used.
  - Customers are responsible for training users on the use and disclosure of passwords used to authenticate to GCP.
  - Customers are responsible for assigning responsibilities for the operation and monitoring of GCP.
  - Customers are responsible for configuring GCP Marketplace permissions in GCP consistent with customers' internal policies. (GCP Marketplace contains enterprise applications that can be added to GCP.)
  - Customers are responsible for restricting access to and monitoring the use of APIs available in GCP.
  - Customers are responsible for enabling, logging, and monitoring functionalities to detect administrator activity, customer support activity, security events, system errors, and data deletions to support customer incident management processes.
  - Customers are responsible for configuring domain settings related to integration with other systems within the customer's environment consistent with customer policies.
  - Customers are responsible for configuring GCP mobile device options consistent with customer policies and procedures.
  - Customers are responsible for the deployment, configuration, and modification of default security settings for GCP products, including VMs, in accordance with their information security requirements.
  - Customers are responsible for enabling logging and monitoring functionalities in their instances of Google Cloud Platform and Multi-Cloud Service Third-Party Provider environments to detect administrator activity, customer support activity, security events, system errors, and data deletions to support customer incident management processes.
- Change Management
  - Customers are responsible for ensuring that individuals creating and/or updating profiles or changing the product configurations are authorized.
  - Customers are responsible for ensuring any application software that they deploy onto GCP follows their specific software change management policies and procedures.

bernard@hotmaker.io

  - Customers are responsible for reviewing and testing features, builds, and product releases, including APIs, to evaluate their impact prior to deploying into production environments, as applicable.
  - Customers are responsible for ensuring that user data is exported and deleted from GCP before or within a reasonable amount of time after termination.
  - Customers are responsible for configuring test and/or development environments in their instance of GCP, as applicable, and restricting access to data in these environments.
  - Customers are responsible for periodically reviewing the configuration of GCP to ensure it is consistent with their policies and procedures.
  - Customers are responsible for configuring external encryption over at-rest storage within their instances of Multi-Cloud Service Third-Party Provider environments to protect their data.
- Physical Security
  - Customers are responsible for ensuring the appropriate physical security controls are established over all devices that access GCP.
  - Customers are responsible for ensuring any devices containing customer data are properly handled, secured, and transported as defined by the product's requirements.
- Incident Management
  - Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of GCP.
  - Customers should train administrators and end users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of GCP.
  - Customers should contact Google if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account, compromise of data, and security events.
- Availability
  - Customers are responsible for ensuring they have business recovery and backup procedures over their non-Google-managed information systems that access GCP.
  - Customers are responsible for configuring data storage locations that support their business and operational resiliency requirements.

bernard@hotmail.fr

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from April 1, 2024 to March 31, 2025.

The Applicable Cloud Computing Compliance Criteria Catalogue (C5) Criteria and Related Controls

The C5 criteria that are in scope for the purposes of this report are as follows:

No.	Area (identifier)	Objective
5.1	Organization of Information Security (OIS)	Plan, implement, maintain, and continuously improve the information security framework within the organization.
5.2	Security Policies and Instructions (SP)	Provide policies and instructions regarding security requirements and support business requirements.
5.3	Personnel (HR)	Ensure that employees understand their responsibilities and are aware of their responsibilities regarding information security and that the organization's assets are protected in the event of changes in responsibilities or termination.
5.4	Asset Management (AM)	Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.
5.5	Physical Security (PS)	Prevent unauthorized physical access and protect against theft, damage, loss, and outage of operations.
5.6	Operations (OPS)	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging, and monitoring events, and dealing with vulnerabilities, malfunctions, and failures.
5.7	Identity and Access Management (IDM)	Secure the authorization and authentication of users of the cloud service provider (typically privileged users) to prevent unauthorized access.
5.8	Cryptography and Key Management (CRY)	Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity, or integrity of information.
5.9	Communication Security (COS)	Ensure the protection of information in networks and the corresponding information processing systems.
5.10	Portability and Interoperability (PI)	Enable the ability to access the cloud service, via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the cloud service provider.
5.11	Procurement, Development and Modification of Information Systems (DEV)	Ensure information security in the development cycle of cloud service system components.
5.12	Control and Monitoring of Service Providers and Suppliers (SSO)	Ensure the protection of information that service providers or suppliers of the cloud service provider (subservice provider) can access and monitor the agreed services and security requirements.

bernard@bernard.io

No.	Area (identifier)	Objective
5.13	Security Incident Management (SIM)	Ensure a consistent and comprehensive approach to the capturing, evaluation, communication, and handling of security incidents.
5.14	Business Continuity Management (BCM)	Plan, implement, maintain, and test procedures and measures for business continuity and emergency management.
5.15	Compliance (COM)	Avoid noncompliance with legal, regulatory, self-imposed, or contractual information security and compliance requirements.
5.16	Dealing with Investigation Requests from Government Agencies (INQ)	Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.
5.17	Product Safety and Security (PSS)	Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, and authentication and authorization of users of cloud customers.

C5 Criteria Not Applicable for GCP

The C5 basic criteria under the objective listed below were determined not to be applicable to Google Cloud Platform, as it does not use traditional backup and recovery mechanisms and achieves data redundancy through replication across multiple clusters within Cloud Regions. This removes the need for traditional backup monitoring or recovery testing mechanisms.

- 5.6: Operations (OPS) criteria OPS-06, OPS-07 and OPS-08

Google's applicable controls supporting the C5 basic criteria are included in Section 4 of this report. Although the applicable criteria and related controls are included in Section 4, they are an integral part of Google's description of its system.

bernard@dotmarket.io

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company's cloud products are serviced from a combination of data centers that are owned by Google and those that are owned by third-party colocation service providers ("subservice organizations"). The Company's controls cover all elements of the Google-owned data centers. For third-party-owned data centers, the Company's controls related to Google Cloud Platform cover only a portion of the overall internal control for each user entity of GCP. The description provided in Physical Access – Data Center Physical Security does not extend to the colocation services for IT infrastructure provided by the subservice organizations. Section 4 of this report and the description of the system only cover the C5 Criteria and related controls of the Company and exclude the related controls of the subservice organizations.

Although the subservice organizations have been carved out for the purposes of this report, certain C5 criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as

backup, recovery, and redundancy controls related to availability. The subservice organizations' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. Subservice organizations' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management monitors the services performed by subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreements, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to subservice organizations management.

It is not feasible for the C5 criteria related to GCP to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at subservice organizations as described below.

Criteria	Complementary Subservice Organization Controls
PS-01, PS-02, PS-03, PS-04, PS-05, PS-06, PS-07	All third-party colocation providers have some responsibility for preventing unauthorized physical access and protecting against theft, damage, and outage of operations. Specific CSOCs that third party colocation providers are responsible for, in addition to monitoring controls performed by the Company, are described in Section 4 of this report.

BigQuery Omni

CSOCs also apply to Google-Managed Multi-Cloud Services, as listed in the Google Cloud Platform Services Summary (https://cloud.google.com/terms/services) (as of the date of this report).

Although the subservice organizations have been carved out for the purposes of this report, certain C5 criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at each of the subservice organizations related to logical and physical security, change management, incident management, and environmental protection, as well as backup, recovery, and redundancy controls related to availability. Subservice organizations (Multi-Cloud Service Third-Party Providers) are listed in the Multi-Cloud Service Third-Party Providers Terms Directory (https://cloud.google.com/terms/mcs-providers) (as of the date of this report) and currently include the following:

- AWS
- Azure

Subservice organizations' logical security and change management controls should mitigate the risk of unauthorized access to the backend infrastructure hosting Google-managed environments. Subservice organizations' physical security controls should mitigate the risk of fires, power loss, climate, and temperature variabilities. Company management receives and reviews the subservice organizations' SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively.

Management also communicates with the subservice organizations to monitor compliance with the service agreements, stay informed of changes planned at the hosting facilities, or relay any issues or concerns to the subservice organizations' management.

bernard@otmake.io

It is not feasible for the C5 criteria related to Google-Managed Multi-Cloud Services to be achieved solely by Google. Therefore, each user entity's internal control must be evaluated in conjunction with Google's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs listed below that are expected to be implemented at subservice organizations:

- 5.5: Physical Security (PS) criteria: PS-01, PS-02, PS-03, PS-04, PS-05, PS-06, and PS-07
- 5.6: Operations (OPS) criteria: OPS-06, OPS-07, OPS-08, and OPS-09
- 5.14: Business Continuity Management (BCM) criteria: BCM-03 and BCM-04
- 5.17: Product Safety and Security (PSS) criteria: PSS-12

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how GCP was used to provide the service from April 1, 2024 to March 31, 2025.

Report Use

The description does not omit or distort information relevant to GCP while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their own particular needs.

bernard@botmaker.io

Section 4

Presentation of Objectives, Basic Criteria, Assigned Controls, Service Auditor's Tests and Results of Tests

bernard@bottaker.io

Presentation of Objectives, Basic Criteria, Assigned Controls, Service Auditor's Tests and Results of Tests

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OIS-01: Information Security Management Systems (ISMS) The Cloud Service Provider operates an information security management system (ISMS) in accordance with ISO/IEC 27001. The scope of the ISMS covers the Cloud Service Provider's organizational units, locations and procedures for providing the cloud service. The measures for setting up, implementing, maintaining and continuously improving the ISMS are documented. The documentation includes: • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and • Results of the last management review (Section 9.3).		
Company goals and responsibilities are required to be developed and communicated by management on a periodic basis and amended as needed. Results are evaluated and communicated to employees.	Inspected the management review of the Information Security Management System (ISMS) report, the Company's Objectives and Key Results (OKR) documentation, and Company newsletters to determine that Company goals and responsibilities were developed and communicated by management at least annually and amended as needed and that results were evaluated and communicated to employees.	No exceptions noted.
The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	Inspected the organization's security policies and procedures to determine that they addressed security, confidentiality, and availability; had been approved by management; and complied with ISO 27001.	No exceptions noted.
	Inspected the organization's intranet accessible to all employees to determine that the organization had policies addressing security, confidentiality, and availability that had been communicated to employees.	No exceptions noted.

bernard@botmaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	Inspected the organization's security policies and procedures to determine that the organization defined information security responsibilities for all employees, delegated decisions on risk identification and resource prioritization to various engineering groups and assigned responsibilities to the Information Security team.	No exceptions noted.
	Inspected the risk assessment to determine that the organization managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly supported the operation of the organization's products and services.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@dmaker.in

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OIS-02: Information Security Policy The top management of the Cloud Service Provider has adopted an information security policy and communicated it to internal and external employees as well as cloud customers. The policy describes: • The importance of information security, based on the requirements of cloud customers in relation to information security; • The security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; • The most important aspects of the security strategy to achieve the security objectives set; and • The organizational structure for information security in the ISMS application area.		
The organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	Inspected the Cloud Data Processing Addendum (CDPA) and the Google Cloud Marketplace PIPA to determine that the organization required external partners to meet security and privacy requirements for safeguarding user data, and that requirements were enforced via the PIPA.	No exceptions noted.
	Inspected the Inbound Service Agreement (ISA) and the Subprocessor Data Processing Agreement (SDPA) for a sample of processors and sub-processors supporting in-scope systems to determine that the organization had implemented a contractual addendum with processors and sub-processors.	No exceptions noted.
	Inspected the termination clause for service issues related to vendors within an example IPA and an example SDPA to determine that it defined the security obligations that processors (including sub-processors) had to meet to satisfy the organization's obligations regarding customer data.	No exceptions noted.

bernard@bolmarc.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The Privacy, Safety Security Org (PSS) takes a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	Inspected the Vendor Security Assessment (VSA) Guidelines to determine that the PSS had a documented, risk-based approach for reviewing vendor security practices and product security posture, including automated procedures for system configuration, performance, response times, and incident recovery.	No exceptions noted.
	Inspected the VSA review documentation, Quarterly Business Reviews (QBRs), and Monthly Business Reports (MBRs) for a sample of vendors to determine that both automated and manual assessments were performed based on data sensitivity.	No exceptions noted.
The organization requires subprocessors to meet security and privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements or other data processing terms.	Inspected the SDPA to determine that the organization required subprocessors to meet security and privacy requirements for safeguarding customer and service data, which were enforced via the SDPA addendum to contractual agreements or other data processing terms.	No exceptions noted.
The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	Inspected the organization's security policies and procedures to determine that they addressed security, confidentiality, and availability; had been approved by management; and complied with ISO 27001.	No exceptions noted.
	Inspected the organization's intranet accessible to all employees to determine that the organization had policies addressing security, confidentiality, and availability that had been communicated to employees.	No exceptions noted.

bernard@trademaker.ro

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	Inspected the organization's security policies and procedures to determine that the organization defined information security responsibilities for all employees, delegated decisions on risk identification and resource prioritization to various engineering groups and assigned responsibilities to the Information Security team.	No exceptions noted.
	Inspected the risk assessment to determine that the organization managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly supported the operation of the organization's products and services.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@formaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OIS-03: Interfaces and Dependencies Interfaces and dependencies between cloud service delivery activities performed by the Cloud Service Provider and activities performed by third parties are documented and communicated. This includes dealing with the following events: • Vulnerabilities; • Security incidents; and • Malfunctions. The type and scope of the documentation is geared towards the information requirements of the subject matter experts of the affected organization's in order to carry out the activities appropriately (e.g. definition of roles and responsibilities in guidelines, description of cooperation obligations in service descriptions and contracts). The communication of changes to the interfaces and dependencies takes place in a timely manner so that the affected organization's and third parties can react appropriately with organizational and technical measures before the changes take effect.		
The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
	Inspected NDA acknowledgements for a sample of external parties to determine that the organization established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.
The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Inspected the Google Cloud Platform (GCP) ToS to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications such as the ToS.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications.	No exceptions noted.

bernard@batmaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Changes to customer facing services that may affect confidentiality, processing integrity and/or availability are communicated to relevant personnel and impacted customers.	Inspected alert notifications and change ticket communication history for a sample of changes to customer-facing services to determine that relevant personnel were notified of changes that could have affected security, confidentiality, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker web page, and the customer-facing log of vulnerabilities to determine that impacted customers were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.
Customer responsibilities are described on the organization's product websites or in system documentation.	Inspected customer responsibilities on the organization's websites and in system documentation, as well as the GCP ToS, that was accessible by internal and external customers to determine that customer responsibilities were described on the organization's product websites or in system documentation.	No exceptions noted.
The organization has implemented a formal reporting structure that is made available to personnel.	Inspected organizational charts and the functional reporting structure made available to personnel on the Company's intranet to determine that the organization had implemented a formal reporting structure that was made available to personnel.	No exceptions noted.
	Inspected management's succession and contingency plans for assignments of responsibility within organizational charts and functional reporting structures to determine that the organization had implemented a formal reporting structure that was made available to personnel.	No exceptions noted.

bernard@tomoker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has policies and guidelines that govern the acceptable use of information assets.	Inspected the defined goals, roles, responsibilities, department coordination requirements, and the safeguards in the Data Security Policy, Data Classification Guidelines, and Code of Conduct to determine that the organization had established policies and guidelines that governed the acceptable use of information assets.	No exceptions noted.
	Inspected the organizational and technical safeguards used by the Company to protect data, IT applications, and IT infrastructure under the Data Security Policy to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.
The organization provides external users with mechanisms to report security issues, incidents and concerns.	Inspected Google support documentation and external support resources to determine that the organization provided external users with mechanisms to report security issues, incidents, and concerns.	No exceptions noted.
The organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	Inspected the CDPA and the Google Cloud Marketplace PIPA to determine that the organization required external partners to meet security and privacy requirements for safeguarding user data, and that requirements were enforced via the PIPA.	No exceptions noted.
	Inspected the ISA and the SDPA for a sample of processors and sub-processors supporting in-scope systems to determine that the organization had implemented a contractual addendum with processors and sub-processors.	No exceptions noted.

bernard@tomaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the termination clause for service issues related to vendors within an example IPA and an example SDPA to determine that it defined the security obligations that processors (including sub-processors) had to meet to satisfy the organization's obligations regarding customer data.	No exceptions noted.
OIS-04: Segregation of Duties Conflicting tasks and responsibilities are separated based on an OIS-06 risk assessment to reduce the risk of unauthorized or unintended changes or misuse of cloud customer data processed, stored, or transmitted in the cloud service. The risk assessment covers the following areas, insofar as these are applicable to the provision of the Cloud Service and are in the area of responsibility of the Cloud Service Provider: • Administration of rights profiles, approval and assignment of access and access authorizations (cf. IDM-01); • Development, testing, and release of changes (cf. DEV-01); and • Operation of the system components. If separation cannot be established for organizational or technical reasons, measures are in place to monitor the activities in order to detect unauthorized or unintended changes as well as misuse and to take appropriate actions.		
The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege.	Inspected the Account Security Policy and the Identity and Access Management Policy to determine that access to information resources, including data and the systems that stored or processed data, was required to be authorized based on the principle of least privilege.	No exceptions noted.
The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment periodically to identify and evaluate risks.	No exceptions noted.

bernard@bormaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the risk assessment documentation to determine that the organization's risk assessment considered the operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
	Inspected the Identity and Access Management Policy and risk assessment documentation to determine that a risk assessment was documented and evaluated the following risk areas: • Administration of rights profiles, approval and assignment of access, and access authorizations • Development, testing, and release of changes • Operation of the system components	No exceptions noted.
	Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas: • Processing, storage, and transmission of data of cloud customers with different protection needs • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources • Attacks via access points, including interfaces accessible from public networks • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons • Dependencies on subservice organizations	No exceptions noted.

bernard@tomaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
System changes are reviewed and approved by a separate technical resource before moving into production.	Inspected change request tickets for a sample of system changes to determine that system changes were documented, tested, reviewed, and approved by a separate technical resource before moving into production.	No exceptions noted.
The organization separates duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	Inspected the Identity and Access Management Policy to determine that the organization separated duties by granting users access based on job responsibilities and least privilege by limiting access to only authorized users.	No exceptions noted.
	Observed an attempt to access a privileged system outside the user's job responsibilities to determine that the organization's separation of duties and principle of least privilege successfully limited access to authorized users only.	No exceptions noted.
Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	Inspected access control lists and the configuration for group administrator approval requirements enforced by the access control system prior to provisioning user access to system components to determine that access to production machines, support tools, and network devices was managed via access control lists and that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
	Inspected the access control management tool history log, tool configuration, and examples of a new hire and transferred employee to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.

bernard@netmaker.ro

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.
	Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.

bernard@ormakar.ro

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OIS-05: Contact with Relevant Government Agencies and Interest Groups The Cloud Service Provider leverages relevant authorities and interest groups in order to stay informed about current threats and vulnerabilities. The information flows into the procedures for handling risks (cf. OIS-06) and vulnerabilities (cf. OPS-19).		
The organization is an active participant in the security industry and maintains appropriate contacts with special interest groups, security forums, and professional associations.	Inspected the Company intranet, an example email notification from the National IT Situation Center and Computer Emergency Response Team (CERT) Association of the Federal Office for Information Security (BSI) (German: Bundesamt für Sicherheit in der Informationstechnik), along with the BSI IT daily situation report and the Google Cloud Security Overview and BSI C5 Security Compliance external web pages to determine that the organization was an active participant in the security industry and maintained appropriate contacts with special interest groups, security forums, professional associations, the National IT Situation Center, and the CERT Association of the BSI.	No exceptions noted.
	Inspected the Google Security Overview external web page to determine that the organization leveraged the information about current threats and vulnerabilities from relevant authorities and interest groups to update procedures for handling risks and vulnerabilities.	No exceptions noted.
The approach to meeting relevant statutory, regulatory, and contractual requirements is defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	Inspected the product launch process, the relevant Google Cloud ToS, and the internal cloud compliance website to determine that the organization's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	No exceptions noted.

bernard@ormuco.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OIS-06: Risk Management Policy Policies and instructions for risk management procedures are documented, communicated and provided in accordance with SP-01 for the following aspects: • Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners; • Analysis of the probability and impact of occurrence and determination of the level of risk; • Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritization of handling; • Handling of risks through measures, including approval of authorization and acceptance of residual risks by risk owners; and • Documentation of the activities implemented to enable consistent, valid and comparable results.		
The organization develops and maintains a risk management framework to manage risk to an acceptable level.	Inspected the risk management guidelines to determine that the organization developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
	Inspected risk management guidelines and the risk assessment documentation to determine that management of the organization evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by management.	Inspected the annual risk assessment and tickets to determine that, as part of the annual risk assessment, risks were mitigated to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.

bernard@bottmaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
OIS-07: Application of the Risk Management Policy The Cloud Service Provider executes the process for handling risks as needed or at least once a year. The following aspects are taken into account when identifying risks, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider: • Processing, storage or transmission of data of cloud customers with different protection needs; • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources; • Attacks via access points, including interfaces accessible from public networks; • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons; and • Dependencies on subservice organization. The analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, is reviewed for adequacy at least annually by the risk owners.		
The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment periodically to identify and evaluate risks.	No exceptions noted.

bernard@tomaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the risk assessment documentation to determine that the organization's risk assessment considered the operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
	Inspected the Identity and Access Management Policy and risk assessment documentation to determine that a risk assessment was documented and evaluated the following risk areas: • Administration of rights profiles, approval and assignment of access, and access authorizations • Development, testing, and release of changes • Operation of the system components	No exceptions noted.
	Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas: • Processing, storage, and transmission of data of cloud customers with different protection needs • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources • Attacks via access points, including interfaces accessible from public networks • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons • Dependencies on subservice organizations	No exceptions noted.

bernard@tomaker.io

5.1 Organization of Information Security (OIS): Plan, implement, maintain and continuously improve the information security framework within the organization.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
System changes are reviewed and approved by a separate technical resource before moving into production.	Inspected change request tickets for a sample of system changes to determine that system changes were documented, tested, reviewed, and approved by a separate technical resource before moving into production.	No exceptions noted.
The organization separates duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	Inspected the Identity and Access Management Policy to determine that the organization separated duties by granting users access based on job responsibilities and least privilege by limiting access to only authorized users.	No exceptions noted.
	Observed an attempt to access a privileged system outside the user's job responsibilities to determine that the organization's separation of duties and principle of least privilege successfully limited access to authorized users only.	No exceptions noted.
The organization develops and maintains a risk management framework to manage risk to an acceptable level.	Inspected the risk management guidelines to determine that the organization developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
	Inspected risk management guidelines and the risk assessment documentation to determine that management of the organization evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.

bernard@metmaker.ro

5.2 Security Policies and Instructions (SP): Provide policies and instructions regarding security requirements and to support business requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
SP-01: Documentation, Communication and Provision of Policies and Instructions Policies and instructions (incl. concepts and guidelines) are derived from the information security policy and are documented according to a uniform structure. They are communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner. The policies and instructions are version controlled and approved by the top management of the Cloud Service Provider or an authorized body. The policies and instructions describe at least the following aspects: • Objectives; • Scope; • Roles and responsibilities, including staff qualification requirements and the establishment of substitution rules; • Roles and dependencies on other organizations (especially cloud customers and subservice organizations); • Steps for the execution of the security strategy; and • Applicable legal and regulatory requirements.		
The organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	Inspected the organization's security policies and procedures to determine that the organization defined information security responsibilities for all employees, delegated decisions on risk identification and resource prioritization to various engineering groups and assigned responsibilities to the Information Security team.	No exceptions noted.
	Inspected the risk assessment to determine that the organization managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly supported the operation of the organization's products and services.	No exceptions noted.
The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	Inspected the organization's security policies and procedures to determine that they addressed security, confidentiality, and availability; had been approved by management; and complied with ISO 27001.	No exceptions noted.

bernard@botmaker.io

5.2 Security Policies and Instructions (SP): Provide policies and instructions regarding security requirements and to support business requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the organization's intranet accessible to all employees to determine that the organization had policies addressing security, confidentiality, and availability that had been communicated to employees.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
The organization has implemented a formal reporting structure that is made available to personnel.	Inspected organizational charts and the functional reporting structure made available to personnel on the Company's intranet to determine that the organization had implemented a formal reporting structure that was made available to personnel.	No exceptions noted.

bernard@hotmaker.ro

5.2 Security Policies and Instructions (SP): Provide policies and instructions regarding security requirements and to support business requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected management's succession and contingency plans for assignments of responsibility within organizational charts and functional reporting structures to determine that the organization had implemented a formal reporting structure that was made available to personnel.	No exceptions noted.
SP-02: Review and Approval of Policies and Instructions Information security policies and instructions are reviewed at least annually for adequacy by the Cloud Service Provider's subject matter experts. The review shall consider at least the following aspects: • Organizational and technical changes in the procedures for providing the cloud service; and • Legal and regulatory changes in the Cloud Service Provider's environment. Revised policies and instructions are approved before they become effective.		
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@botmaker.io

5.2 Security Policies and Instructions (SP): Provide policies and instructions regarding security requirements and to support business requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
SP-03: Exceptions from Existing Policies and Instructions Exceptions to the policies and instructions for information security as well as respective controls go through the OIS-06 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of exceptions are documented, limited in time and are reviewed for appropriateness at least annually by the risk owners.		
The organization has established a process to review and approve requests for policy exceptions.	Inspected the Security and Privacy Policy Creation and Maintenance document and the Policy Exceptions internal web page to determine that the organization had documented the established policy exception process to ensure that a formal approval and risk evaluation were performed.	No exceptions noted.
	Inspected the tracking bug tickets and management approvals for a sample of policy exception requests to determine that the organization had established the policy exception process to ensure that a formal approval and risk evaluation were performed.	No exceptions noted.

bernard@bornaker.io

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
HR-01: Verification of Qualification and Trustworthiness The competency and integrity of all internal and external employees of the Cloud Service Provider with access to cloud customer data or system components under the Cloud Service Provider's responsibility who are responsible to provide the cloud service in the production environment shall be verified prior to commencement of employment in accordance with local legislation and regulation by the Cloud Service Provider. To the extent permitted by law, the review will cover the following areas: • Verification of the person through identity card; • Verification of the CV; • Verification of academic titles and degrees; • Request of a police clearance certificate for applicants; • Certificate of good conduct or national equivalent; and • Evaluation of the risk to be blackmailed.		
Background checks are performed on new hires as permitted by local laws.	Inspected the guidelines for the hiring process to determine that background checks were required to be performed on new employees, temporary workers, and independent contractors, in compliance with local laws, upon hire.	No exceptions noted.
	Inspected background check documentation for a sample of new employees, temporary workers, and independent contractors to determine that background checks were performed as required for all new members of the organization, in compliance with local laws, upon hire.	No exceptions noted.
New hires or internal transfers are required to go through an official recruiting process during which they are screened against detailed job descriptions and interviewed to assess competence.	Inspected onboarding records and job descriptions for a sample of new hires and internal transfers to determine that new hires and internal transfers were required to go through an official recruiting process, during which they were screened against detailed job descriptions and interviewed to assess competence.	No exceptions noted.

bernard@botmaker.io

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
HR-02: Employment Terms and Conditions The Cloud Service Provider's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security. The information security policy, and the policies and instructions based on it, are to be acknowledged by the internal and external personnel in a documented form before access is granted to any cloud customer data or system components under the responsibility of the Cloud Service Provider used to provide the cloud service in the production environment.		
The organization has established a code of conduct that is reviewed and updated as needed.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Data Security Policy, and Security and Resilience Policy to determine that the organization had established internal privacy and information security policies, as well as a Code of Conduct, that were reviewed and updated as needed.	No exceptions noted.
Personnel of the organization are required to acknowledge the code of conduct.	Inspected acknowledgements of the Code of Conduct and information security policies for a sample of new hire employees, temporary workers, and independent contractors to determine that employees and members of the extended workforce were required to acknowledge the Code of Conduct upon hire.	No exceptions noted.
The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected the confidentiality agreement template to determine that the organization had established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	No exceptions noted.

bernard@coalfire.com

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected confidentiality agreement acknowledgements for a sample of extended workforce personnel to determine that extended workforce personnel acknowledged the organization's established confidentiality agreements, which defined responsibilities and expected behavior for the protection of information.	No exceptions noted.
The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inspected employee responsibilities and expected behavior for the protection of information within the confidentiality agreement template and Code of Conduct to determine that the organization established confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of employees to determine that employees acknowledged the organization's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information upon employment.	No exceptions noted.
HR-03: Security Training and Awareness Program The Cloud Service Provider operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the Cloud Service Provider on a regular basis. The program is regularly updated based on changes to policies and instructions and the current threat situation and includes the following aspects: • Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; • Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behavior in the event of security incidents.		

bernard@hofmeker.io

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.	Inspected the privacy and information security training content on tools, standards, and methods of secure software development and provisioning to determine that the organization provided annual training programs for both internal and external employees, focusing on secure software development practices and tool usage.	No exceptions noted.
	Inspected the compliance monitoring tool dashboard used by management to track employees' completion rates for required privacy and information security awareness training, configurations for the automated training enrollment tool, and an example of an email notification for overdue training to determine that the organization had established a privacy and information security training program covering both quantitative and qualitative measurements and that relevant personnel met the annual training completion requirements.	No exceptions noted.
	Inspected the privacy and information security training program content to determine that the organization reviewed and updated training content at least annually, based on the results achieved through the privacy and information security awareness training program.	No exceptions noted.

bernard@formaker.io

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
HR-04: Disciplinary Measures In the event of violations of policies and instructions or applicable legal and regulatory requirements, actions are taken in accordance with a defined policy that includes the following aspects: • Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact. The internal and external employees of the Cloud Service Provider are informed about possible disciplinary measures. The use of disciplinary measures is appropriately documented.		
The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	Inspected the Code of Conduct and the internal case management system to determine that the organization had established a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.
	Inspected disciplinary case records for a sample of disciplinary incidents to determine that the organization enforced a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.
HR-05: Responsibilities in the Event of Termination or Change of Employment Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.		
The organization has established an offboarding procedure for personnel, which governs the removal of access and return of assets.	Inspected the internal offboarding guidelines to determine that the organization established and communicated offboarding procedures that governed the removal of access and return of assets and that terminated employees and Temps, Vendors, and Contractors (TVCs) were required to return Google property and assets assigned or given during their employment.	No exceptions noted.

bernard@dealmaker.io

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the internal offboarding guidelines to determine that employees and TVCs were informed of their obligations to comply with relevant laws, regulations, and provisions and that information security requirements remained valid even if their responsibilities changed or their employment was terminated.	No exceptions noted.
	Inspected the terminated employee Exit Certification Letter template to determine that all organizational assets in the possession of terminated personnel were requested and required to be returned upon termination, that organizational assets were tracked and returned when possible, and that all confidential authentication data was rendered obsolete during offboarding procedures.	No exceptions noted.
The organization has established a code of conduct that is reviewed and updated as needed.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Data Security Policy, and Security and Resilience Policy to determine that the organization had established internal privacy and information security policies, as well as a Code of Conduct, that were reviewed and updated as needed.	No exceptions noted.
Personnel of the organization are required to acknowledge the code of conduct.	Inspected acknowledgements of the Code of Conduct and information security policies for a sample of new hire employees, temporary workers, and independent contractors to determine that employees and members of the extended workforce were required to acknowledge the Code of Conduct upon hire.	No exceptions noted.

bernard@tomaker.io

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected the confidentiality agreement template to determine that the organization had established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of extended workforce personnel to determine that extended workforce personnel acknowledged the organization's established confidentiality agreements, which defined responsibilities and expected behavior for the protection of information.	No exceptions noted.
The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inspected employee responsibilities and expected behavior for the protection of information within the confidentiality agreement template and Code of Conduct to determine that the organization established confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of employees to determine that employees acknowledged the organization's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information upon employment.	No exceptions noted.

bernard@ormaker.io

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
HR-06: Confidentiality Agreements The non-disclosure or confidentiality agreements to be agreed with internal employees, external service providers and suppliers of the Cloud Service Provider are based on the requirements identified by the Cloud Service Provider for the protection of confidential information and operational details. The agreements are to be accepted by external service providers and suppliers when the contract is agreed. The agreements must be accepted by internal employees of the Cloud Service Provider before authorization to access data of cloud customers is granted. The requirements must be documented and reviewed at regular intervals (at least annually). If the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements are updated. The Cloud Service Provider must inform the internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.		
The organization has established confidentiality agreements that are reviewed (by regional Employment Legal teams) and updated (by Google's regional Offer Letter teams), as needed. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No changes were made to confidentiality agreements during the period that required acknowledgements of the updated versions.	Inspected the ticket evidence of the annual review of confidentiality agreements for employees and information-sharing agreements with third parties, vendors, individuals, and businesses to determine that confidentiality agreements and information sharing agreements were reviewed annually.	No exceptions noted.
	Inquired with management and inspected the ticket evidence of the annual review of confidentiality agreements for employees and information-sharing agreements with third parties, vendors, individuals, and businesses to determine that the circumstances that warranted the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether changes made to confidentiality agreements during the annual review required acknowledgements of the updated versions.	Not tested. No changes were made to confidentiality agreements during the period that required acknowledgements of the updated versions.

kamerd@hotmail.io

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected the confidentiality agreement template to determine that the organization had established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of extended workforce personnel to determine that extended workforce personnel acknowledged the organization's established confidentiality agreements, which defined responsibilities and expected behavior for the protection of information.	No exceptions noted.
The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inspected employee responsibilities and expected behavior for the protection of information within the confidentiality agreement template and Code of Conduct to determine that the organization established confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of employees to determine that employees acknowledged the organization's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information upon employment.	No exceptions noted.
The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the nondisclosure agreement (NDA) templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.

bernard@hotmaker.jp

5.3 Personnel (HR): Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected NDA acknowledgements for a sample of external parties to determine that the organization established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.

bernard@botmaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
AM-01: Asset Inventory The Cloud Service Provider has established procedures for inventorying assets. The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle. Assets are recorded with the information needed to apply the Risk Management Procedure (cf. OIS-07), including the measures taken to manage these risks throughout the asset lifecycle. Changes to this information are logged.		
Automated mechanisms are utilized to track inventory of all production machines and inventory of all serialized server components.	Inspected the Device Configuration Guidelines to determine that the organization established procedures for automated mechanisms that were utilized to track inventory of production machines.	No exceptions noted.
	Observed production machines during data center inspections for a sample of production machines tracked in the automated inventory management tool to determine that automated mechanisms were utilized to track inventory of production machines.	No exceptions noted.
	Inspected production machines tracked in the automated inventory management tool for a sample of production machines observed during data center inspections to determine that automated mechanisms were utilized to track inventory of production machines.	No exceptions noted.
	Inspected asset event history logs and the asset event monitoring tool that detected events and automatically updated the inventory management tool to determine that automated mechanisms were utilized to track inventory of all production machines and inventory of all serialized server components.	No exceptions noted.

bernard@bonnaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The Technical Infrastructure Product Area ultimately owns assets used for information processing (i.e. production machines). Assets are allocated to individual teams upon request.	Inspected the GCP Compute Engine product page to determine that assets used for information processing were owned by the Technical Infrastructure Product Area and were able to be allocated to individual teams upon request.	No exceptions noted.
The organization has established mechanisms governing the configuration and security of corporate-managed CrOS, Android and iOS devices providing privileged access.	Inspected the global policy configuration of antivirus, antimalware, and antispam tools installed on each in-scope operating system type to determine that the organization had established mechanisms that governed the security of corporate-managed devices that provided privileged access.	No exceptions noted.
	Inspected the configurations for the software management systems that installed software and tracked usage to determine that the organization had established mechanisms that governed the configuration of corporate-managed devices that provided privileged access.	No exceptions noted.
The organization maintains an up-to-date, accurate client device inventory.	Inspected the procedures for inventorying assets and an example of the client asset inventory review performed to determine that the organization maintained an updated, accurate, and consistent client device inventory throughout the asset lifecycle.	No exceptions noted.
The organization has policies and guidelines that govern the acceptable use of information assets.	Inspected the defined goals, roles, responsibilities, department coordination requirements, and the safeguards in the Data Security Policy, Data Classification Guidelines, and Code of Conduct to determine that the organization had established policies and guidelines that governed the acceptable use of information assets.	No exceptions noted.

bernard@battmaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the organizational and technical safeguards used by the Company to protect data, IT applications, and IT infrastructure under the Data Security Policy to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.
AM-02: Acceptable Use and Safe Handling of Assets Policy Policies and instructions for acceptable use and safe handling of assets are documented, communicated and provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset: • Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorized personnel or system components; • Inventory; • Classification and labeling based on the need for protection of the information and measures for the level of protection identified; • Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorization; • Requirements for versions of software and images as well as application of patches; • Handling of software for which support and security patches are not available anymore; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Physical delivery and transport; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.		
The organization has policies and guidelines governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy, the Security Requirements for Outsourced Software Development Policy, and the Source Code Guidelines, to determine that the organization had established policies and guidelines governing the secure development lifecycle, including requirements for outsourced development.	No exceptions noted.

bernard@bormaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with the data retention and deletion policy.	No exceptions noted.
	Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	Inspected the organization's Cryptographic Policy and the CDPA web page available to external users to determine that encryption mechanisms were required and communicated to protect user authentication and administrator sessions transmitted over the Internet.	No exceptions noted.
	Inspected server scan results and encryption configurations and observed user administrator connection settings to determine that encryption mechanisms were used to protect user authentication and administrator sessions transmitted over the Internet.	No exceptions noted.
The organization has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the Cryptographic Policy and Key Management Policy to determine that an established key management process was in place to support the organization's use of cryptographic techniques.	No exceptions noted.

bernard@hotmaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the code configuration for enforcing encryption, certificate authentication, and revocation to determine that an established key management process supported the organization's use of cryptographic techniques.	No exceptions noted.
The organization has policies and guidelines in place which govern the use of intellectual property and third-party software. The organization utilizes software management systems to install software and track usage.	Inspected the Software Development Life Cycle (SDLC) policy and software management systems to determine that the organization had policies and guidelines in place governing the use of intellectual property and third-party software and that it utilized software management systems to install software and track usage.	No exceptions noted.
The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	Inspected the Mobile Device Support Policy and Mobile Device Security Guidelines to determine that the organization-maintained policies and guidelines for securing mobile devices used to access the corporate networks and systems.	No exceptions noted.
The organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the CDPA, Data Security Policy, Security Classification Labeling Guidelines, and the Data Categorization Guidelines to determine that the organization had established policies and guidelines to define customer data and govern data classification, labeling, and security and that the organization's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and updated at least annually.	No exceptions noted.

bernard@dotmaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the documented safeguards in the Data Security Policy and the guidance provided to product teams on handling metadata to determine that the organization defined and implemented rules for the collection, access, processing, handling, retention, and deletion of metadata.	No exceptions noted.
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the network guidelines, production image enforcement tool configurations, customer image restriction cloud portal functionality, and default hardening standards for machines and containers to determine that virtual environments were hardened where the organization held a responsibility as outlined in the shared responsibilities and mechanisms were provided for restricting the selection of default hardened images for virtual machines and containers in the cloud environment.	No exceptions noted.
The organization has established a code of conduct that is reviewed and updated as needed.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Data Security Policy, and Security and Resilience Policy to determine that the organization had established internal privacy and information security policies, as well as a Code of Conduct, that were reviewed and updated as needed.	No exceptions noted.
The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected the confidentiality agreement template to determine that the organization had established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	No exceptions noted.

bernard@...ormaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected confidentiality agreement acknowledgements for a sample of extended workforce personnel to determine that extended workforce personnel acknowledged the organization's established confidentiality agreements, which defined responsibilities and expected behavior for the protection of information.	No exceptions noted.
The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inspected employee responsibilities and expected behavior for the protection of information within the confidentiality agreement template and Code of Conduct to determine that the organization established confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of employees to determine that employees acknowledged the organization's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information upon employment.	No exceptions noted.
The organization has policies and guidelines that govern the acceptable use of information assets.	Inspected the defined goals, roles, responsibilities, department coordination requirements, and the safeguards in the Data Security Policy, Data Classification Guidelines, and Code of Conduct to determine that the organization had established policies and guidelines that governed the acceptable use of information assets.	No exceptions noted.

bernard@...maker.in

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the organizational and technical safeguards used by the Company to protect data, IT applications, and IT infrastructure under the Data Security Policy to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
The organization has established mechanisms governing the configuration and security of corporate-managed CrOS, Android and iOS devices providing privileged access.	Inspected the global policy configuration of antivirus, antimalware, and antispam tools installed on each in-scope operating system type to determine that the organization had established mechanisms that governed the security of corporate-managed devices that provided privileged access.	No exceptions noted.

bernard@dronker.nl

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the configurations for the software management systems that installed software and tracked usage to determine that the organization had established mechanisms that governed the configuration of corporate-managed devices that provided privileged access.	No exceptions noted.
AM-03: Commissioning of Hardware The Cloud Service Provider has an approval process for the use of hardware to be commissioned, which is used to provide the cloud service in the production environment, in which the risks arising from the commissioning are identified, analyzed and mitigated. Approval is granted after verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorization according to the intended use and based on the applicable policies.		
Changes to the organization's systems are tested before being deployed.	Inspected testing notes within change request tickets for a sample of system changes to determine that changes to the organization's systems were tested prior to deployment.	No exceptions noted.
Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	Inspected access control lists and the configuration for group administrator approval requirements enforced by the access control system prior to provisioning user access to system components to determine that access to production machines, support tools, and network devices was managed via access control lists and that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
	Inspected the access control management tool history log, tool configuration, and examples of a new hire and transferred employee to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.

bernard@bornaker.no

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the network guidelines, production image enforcement tool configurations, customer image restriction cloud portal functionality, and default hardening standards for machines and containers to determine that virtual environments were hardened where the organization held a responsibility as outlined in the shared responsibilities and mechanisms were provided for restricting the selection of default hardened images for virtual machines and containers in the cloud environment.	No exceptions noted.
The organization has policies and guidelines governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy, the Security Requirements for Outsourced Software Development Policy, and the Source Code Guidelines, to determine that the organization had established policies and guidelines governing the secure development lifecycle, including requirements for outsourced development.	No exceptions noted.
Automated mechanisms are utilized to track inventory of all production machines and inventory of all serialized server components.	Inspected the Device Configuration Guidelines to determine that the organization established procedures for automated mechanisms that were utilized to track inventory of production machines.	No exceptions noted.
	Observed production machines during data center inspections for a sample of production machines tracked in the automated inventory management tool to determine that automated mechanisms were utilized to track inventory of production machines.	No exceptions noted.

hernard@protonmail.ch

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected production machines tracked in the automated inventory management tool for a sample of production machines observed during data center inspections to determine that automated mechanisms were utilized to track inventory of production machines.	No exceptions noted.
	Inspected asset event history logs and the asset event monitoring tool that detected events and automatically updated the inventory management tool to determine that automated mechanisms were utilized to track inventory of all production machines and inventory of all serialized server components.	No exceptions noted.
AM-04: Decommissioning of Hardware The decommissioning of hardware used to operate system components supporting the cloud service production environment under the responsibility of the Cloud Service Provider requires approval based on the applicable policies. The decommissioning includes the complete and permanent deletion of the data or proper destruction of the media.		
The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with the data retention and deletion policy.	No exceptions noted.
	Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.

bernard@lomaker.in

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
AM-05: Commitment to Permissible Use, Safe Handling and Return of Assets The Cloud Service Provider's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the Cloud Service Provider has determined in a risk assessment that loss or unauthorized access could compromise the information security of the Cloud Service. Any assets handed over are provably returned upon termination of employment.		
The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.	Inspected the User Data Wipeout Policy (UDWP) and Data Destruction Guidelines to determine that the organization sanitized storage media prior to disposal, release from organizational control, or release for reuse.	No exceptions noted.
	Observed destroyed media bins and inspected asset management system records for a sample of data centers to determine that storage media were physically destroyed before disposal, release from organizational control, or release for reuse.	No exceptions noted.
The organization has guidelines in place for the management and use of removable media.	Inspected asset management policies, guidelines, FAQs, and help articles to determine that the organization had guidelines in place for the management and use of removable media.	No exceptions noted.
The organization has mechanisms in place to prevent deactivated or deleted user accounts from being reassigned to new users.	Inspected the user account management processes and configurations, including remote deactivation, deletion, and locking capabilities, to determine that mechanisms were in place to prevent deactivated or deleted user accounts from being reassigned to new users.	No exceptions noted.
Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Inspected the critical access groups' configuration to determine that reviews were assigned to authorized group administrators, ensuring that logical access was restricted to authorized personnel and periodically reviewed.	No exceptions noted.

bernard@hotmail.it

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected a sample of semi-annual user membership reviews for critical access groups, performed by group administrators, to determine that access was appropriately restricted and all review activities were tracked to completion.	No exceptions noted.
	Inspected automatic account revocation configurations to determine that inappropriate access identified during the semi-annual critical access group membership reviews was removed at least hourly.	No exceptions noted.
The organization has established a code of conduct that is reviewed and updated as needed.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Data Security Policy, and Security and Resilience Policy to determine that the organization had established internal privacy and information security policies, as well as a Code of Conduct, that were reviewed and updated as needed.	No exceptions noted.
The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected the confidentiality agreement template to determine that the organization had established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of extended workforce personnel to determine that extended workforce personnel acknowledged the organization's established confidentiality agreements, which defined responsibilities and expected behavior for the protection of information.	No exceptions noted.

bernard@intruder.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inspected employee responsibilities and expected behavior for the protection of information within the confidentiality agreement template and Code of Conduct to determine that the organization established confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of employees to determine that employees acknowledged the organization's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information upon employment.	No exceptions noted.
The organization has established an offboarding procedure for personnel, which governs the removal of access and return of assets.	Inspected the internal offboarding guidelines to determine that the organization established and communicated offboarding procedures that governed the removal of access and return of assets and that terminated employees and TVCs were required to return Google property and assets assigned or given during their employment.	No exceptions noted.
	Inspected the internal offboarding guidelines to determine that employees and TVCs were informed of their obligations to comply with relevant laws, regulations, and provisions and that information security requirements remained valid even if their responsibilities changed or their employment was terminated.	No exceptions noted.

bernard@ormakerio

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the terminated employee Exit Certification Letter template to determine that all organizational assets in the possession of terminated personnel were requested and required to be returned upon termination, that organizational assets were tracked and returned when possible, and that all confidential authentication data was rendered obsolete during offboarding procedures.	No exceptions noted.
The organization has policies and guidelines that govern the acceptable use of information assets.	Inspected the defined goals, roles, responsibilities, department coordination requirements, and the safeguards in the Data Security Policy, Data Classification Guidelines, and Code of Conduct to determine that the organization had established policies and guidelines that governed the acceptable use of information assets.	No exceptions noted.
	Inspected the organizational and technical safeguards used by the Company to protect data, IT applications, and IT infrastructure under the Data Security Policy to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.
The organization has established mechanisms governing the configuration and security of corporate-managed CrOS, Android and iOS devices providing privileged access.	Inspected the global policy configuration of antivirus, antimalware, and antispam tools installed on each in-scope operating system type to determine that the organization had established mechanisms that governed the security of corporate-managed devices that provided privileged access.	No exceptions noted.

bernard@tomaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the configurations for the software management systems that installed software and tracked usage to determine that the organization had established mechanisms that governed the configuration of corporate-managed devices that provided privileged access.	No exceptions noted.
AM-06: Asset Classification and Labeling Assets are classified and, if possible, labeled. Classification and labeling of an asset reflects the protection needs of the information it processes, stores, or transmits. The need for protection is determined by the individuals or groups responsible for the assets of the Cloud Service Provider according to a uniform schema. The schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.		
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	No exceptions noted.
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.

bernard@bonmaker.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.
The organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the CDPA, Data Security Policy, Security Classification Labeling Guidelines, and the Data Categorization Guidelines to determine that the organization had established policies and guidelines to define customer data and govern data classification, labeling, and security and that the organization's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and updated at least annually.	No exceptions noted.
	Inspected the documented safeguards in the Data Security Policy and the guidance provided to product teams on handling metadata to determine that the organization defined and implemented rules for the collection, access, processing, handling, retention, and deletion of metadata.	No exceptions noted.
The organization maintains an up-to-date, accurate client device inventory.	Inspected the procedures for inventorying assets and an example of the client asset inventory review performed to determine that the organization maintained an updated, accurate, and consistent client device inventory throughout the asset lifecycle.	No exceptions noted.

bernard@romaker.ro

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the network guidelines, production image enforcement tool configurations, customer image restriction cloud portal functionality, and default hardening standards for machines and containers to determine that virtual environments were hardened where the organization held a responsibility as outlined in the shared responsibilities and mechanisms were provided for restricting the selection of default hardened images for virtual machines and containers in the cloud environment.	No exceptions noted.
Automated mechanisms are utilized to track inventory of all production machines and inventory of all serialized server components.	Inspected the Device Configuration Guidelines to determine that the organization established procedures for automated mechanisms that were utilized to track inventory of production machines.	No exceptions noted.
	Observed production machines during data center inspections for a sample of production machines tracked in the automated inventory management tool to determine that automated mechanisms were utilized to track inventory of production machines.	No exceptions noted.
	Inspected production machines tracked in the automated inventory management tool for a sample of production machines observed during data center inspections to determine that automated mechanisms were utilized to track inventory of production machines.	No exceptions noted.

bernard@tomtekor.io

5.4 Asset Management (AM): Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected asset event history logs and the asset event monitoring tool that detected events and automatically updated the inventory management tool to determine that automated mechanisms were utilized to track inventory of all production machines and inventory of all serialized server components.	No exceptions noted.

bernard@botmaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
PS-01: Physical Security and Environmental Control Requirements Security requirements for premises and buildings related to the cloud service provided, are based on the security objectives of the information security policy, identified protection requirements for the cloud service and the assessment of risks to physical and environmental security. The security requirements are documented, communicated and provided in a policy or concept according to SP-01. The security requirements for data centers are based on criteria which comply with established rules of technology. They are suitable for addressing the following risks in accordance with the applicable legal and contractual requirements: • Faults in planning; • Unauthorized access; • Insufficient surveillance; • Insufficient air-conditioning; • Fire and smoke; • Water; • Power failure; and • Air ventilation and filtration. If the Cloud Service Provider uses premises or buildings operated by third parties to provide the Cloud Service, the document describes which security requirements the Cloud Service Provider places on these third parties. The appropriate and effective verification of implementation is carried out in accordance with the criteria for controlling and monitoring subcontractors (cf. SSO-01, SSO-02).		
BigQuery Omni is hosted on third-party infrastructure, and physical security and environmental control requirements are the responsibility of the subservice organizations.	Not applicable.	Not applicable.
The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.	Inspected the Business Impact Analysis (BIA) Report; Data Center Access Policy; Third-Party Data Center Physical Security Requirements; Data Center Security Policy; Data Center Photo Policy; Europe, Middle East, and Africa (EMEA) Heating Ventilation and Air Conditioning (HVAC) Design Guidelines; and Environmental Health and Safety (EHS) Owner Project Requirements (OPR) to determine that the organization	No exceptions noted.

bernard@botmaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	had policies and guidelines to keep its physical workplaces, facilities, and property safe, addressing risks from the following: • Faults in planning • Unauthorized access • Insufficient surveillance • Insufficient air conditioning • Fire and smoke • Water • Power failure • Air ventilation and filtration	
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@boilmaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
PS-02: Redundancy Model The cloud service is provided from two locations that are redundant to each other. The locations meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and are located in an adequate distance to each other to achieve operational redundancy. Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met. The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04 - Verification, updating and testing of business continuity).		
BigQuery Omni is hosted on third-party infrastructure, and redundancy model is the responsibility of the subservice organizations.	Not applicable.	Not applicable.
The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the replication tool dashboard; monitoring tool dashboard; and filesystem, datastore, and network configurations for products and networks to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities.	No exceptions noted.
	Inspected the CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of customer data through the implementation of backups within the organization's information processing resources.	No exceptions noted.
The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklists to determine that DR and BC testing was required to be conducted at least annually and included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.

bernard@hotmaker.ro

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected DR and BC testing documentation and results for a sample of products to determine that the organization conducted disaster resiliency testing covering reliability, survivability, and recovery at least annually.	Exception noted. For 1 out of 25 Disaster Resiliency Tests sampled, the organization did not provide sufficient documentation confirming that disaster resiliency testing was conducted on an ongoing basis (at least annually) to adequately cover reliability, survivability, and recovery. An additional sample of 15 Disaster Resiliency Tests was selected and testing was completed for each of the products in the additional sample.
	Inspected the BIA documentation to determine that potential impacts to business operations were considered.	No exceptions noted.
The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	Inspected the BIA, BC planning documentation, and the organization's ISO 27001 Statement of Applicability (SoA) to determine that requirements were established for business continuity measures that maintained the availability of the organization's production infrastructure and services.	No exceptions noted.

bernard@botmaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected Disaster Resiliency Testing documentation, including assigned roles, responsibilities, risks, and recovery objectives within the BC Plan, to determine that the organization implemented business continuity measures to maintain the availability of its production infrastructure and services.	No exceptions noted.
	Inspected documented recovery activities in the DR Report to determine that recovery activities were outlined to maintain the availability of the organization's production infrastructure and services.	No exceptions noted.
PS-03: Perimeter Protection The structural shell of premises and buildings related to the cloud service provided are physically solid and protected by adequate security measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). The security measures are designed to detect and prevent unauthorized access in a timely manner so that it does not compromise the information security of the cloud service. The outer doors, windows and other construction elements reach a level appropriate to the security requirements and withstand a burglary attempt for at least 10 minutes. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.		
BigQuery Omni is hosted on third-party infrastructure, and perimeter protection is the responsibility of the subservice organizations.	Not applicable.	Not applicable.
Data center perimeters are defined and secured via physical barriers.	Observed structural features, including fenced perimeters, doors, walls, and segregated security zones, for a sample of data centers to determine that data center perimeters were defined by physical barriers.	No exceptions noted.

bernard@bormaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Observed locks on doors, security personnel monitoring sensitive data center zones, and security system alerts to determine that data center perimeters were secured through physical security controls.	No exceptions noted.
Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	Observed security personnel monitoring sensitive data center zones through the use of real-time video surveillance for a sample of data centers to determine that sensitive data centers zones were continuously monitored.	No exceptions noted.
	Observed security personnel monitoring facility buildings and campus through real-time video surveillance and inspected guard schedules for a sample of data centers to determine that facility buildings and campus were continuously monitored and staffed by at least two security personnel at all times.	No exceptions noted.
	Observed "forced door tests" on-site and inspected physical access logs corresponding to those tests to determine that data centers were continuously monitored by security personnel using alerts generated by security systems.	No exceptions noted.
Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Inspected documentation of data center security reviews performed for all in-scope data centers to determine that data center security measures were assessed at least annually and the results were reviewed by executive management.	No exceptions noted.

bernard@bonMaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
PS-04: Physical Site Access Control At access points to premises and buildings related to the cloud service provided, physical access controls are set up in accordance with the Cloud Service Provider's security requirements (cf. PS-01 Security Concept) to prevent unauthorized access. Access controls are supported by an access control system. The requirements for the access control system are documented, communicated and provided in a policy or concept in accordance with SP-01 and include the following aspects: • Specified procedure for the granting and revoking of access authorizations (cf. IDM-02) based on the principle of least authorization ("least-privilege-principle") and as necessary for the performance of tasks ("need-to-know principle"); • Automatic revocation of access authorizations if they have not been used for a period of 2 month; • Automatic withdrawal of access authorizations if they have not been used for a period of 6 months; • Two-factor authentication for access to areas hosting system components that process cloud customer information; • Visitors and external personnel are tracked individually by the access control during their work in the premises and buildings, identified as such (e.g., by visible wearing of a visitor pass) and supervised during their stay; and • Existence and nature of access logging that enables the Cloud Service Provider, in the sense of an effectiveness audit, to check whether only defined personnel have entered the premises and buildings related to the cloud service provided.		
BigQuery Omni is hosted on third-party infrastructure, and physical site access control is the responsibility of the subservice organizations.	Not applicable.	Not applicable.
Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.	Inspected policy documentation produced by the Cloud CISO Compliance & Certifications (C4) Team to determine that two-factor authentication access control was required by policy for sensitive data center zones and that facility visitors were, by policy, required to be tracked and escorted during visits.	No exceptions noted.

vernard@otmaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Observed badge readers, secondary identification mechanisms, physical locks, and the enforcement of two-factor authentication for a sample of data centers to determine that two-factor authentication was enforced for access to sensitive data center zones through badge readers, secondary identification mechanisms, and/or physical locks.	No exceptions noted.
	Inspected visitor data center site access request tickets with business-specific approvals for entry to sensitive zones, for a sample of data centers, to determine that access to sensitive zones required approval from authorized personnel.	No exceptions noted.
Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.	Inspected visitor access request tickets and observed the check-in process to determine that visitors were required to gain approval from authorized personnel before entering data center facilities.	No exceptions noted.
	Observed the visitor check-in process and the enforcement of escort requirements for a sample of data centers to determine that visitor identities were verified at facility perimeters and visitors were required to remain with escorts for the duration of their visit.	No exceptions noted.
Data center physical access logs are recorded and retained in accordance with organizational or regulatory requirements.	Inspected the configuration of retention periods for data center physical access logs and example activity log history to determine that data center physical access logs were recorded and retained in accordance with the retention requirements detailed in the corporate retention requirements.	No exceptions noted.

bernard@boilmaker.ro

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.	Inspected documentation of data center access reviews performed for all in-scope data centers to determine that access lists for high-security areas in data centers were reviewed quarterly and inappropriate access was removed in a timely manner.	No exceptions noted.
	Inspected the Data Center Physical Access Policy to determine that access was automatically revoked if a user had not accessed a data center for 2 months and withdrawn if a user had not accessed a data center for 6 months.	Exceptions noted. The organization did not enforce the automatic revocation of data center access after 2 months of inactivity or the automatic removal after 6 months of inactivity.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.

bernard@bottmaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Inspected documentation of data center security reviews performed for all in-scope data centers to determine that data center security measures were assessed at least annually and the results were reviewed by executive management.	No exceptions noted.
PS-05: Protection from Fire and Smoke Premises and buildings related to the cloud service provided are protected from fire and smoke by structural, technical and organizational measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and include the following aspects: a) Structural Measures: • Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts. b) Technical Measures: • Early fire detection with automatic voltage release. The monitored areas are sufficiently fragmented to ensure that the prevention of the spread of incipient fires is proportionate to the maintenance of the availability of the cloud service provided; • Extinguishing system or oxygen reduction; and • Fire alarm system with reporting to the local fire department. c) Organizational Measures • Regular fire protection inspections to check compliance with fire protection requirements; and • Regular fire protection exercises.		
BigQuery Omni is hosted on third-party infrastructure, and protection from fire and smoke is the responsibility of the subservice organizations.	Not applicable.	Not applicable.

bernard@bumraker.ru

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Data centers are equipped with fire detection alarms and protection equipment.	Observed fire suppression systems and automatic voltage-release smoke detectors in sensitive data center zones for a sample of data centers to determine that fire detection alarms and protection equipment were installed.	No exceptions noted.
	Observed evidence of fire drill procedure cadence and fire drill completion documentation for a sample of data centers to determine that fire alarm systems reported to local fire departments.	No exceptions noted.
	Inspected fire rating documentation for a sample of data centers to determine that structural components were rated to maintain integrity for at least 90 minutes.	Exceptions noted. For 3 out of the 8 facilities sampled, the structural components were not constructed with a fire resistance rating of at least 90 minutes.
Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	Inspected maintenance records for a sample of data centers to determine that critical equipment (generators, Uninterruptible Power Supplies [UPS] systems, chillers, fire suppression systems, emergency lighting, and HVAC systems) were continuously monitored and maintained through routine inspections, regular maintenance, and ad-hoc repairs in accordance with organizational requirements.	No exceptions noted.

bernard@hotmaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Observed systems and personnel monitoring climate controls in sensitive data center zones and triggered alerts for a sample of data centers to determine that critical equipment supporting products and services was continuously monitored.	No exceptions noted.
Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Inspected documentation of data center security reviews performed for all in-scope data centers to determine that data center security measures were assessed at least annually and the results were reviewed by executive management.	No exceptions noted.

PS-06: Protection Against Interruptions Caused by Power Failures and Other Such Risks

Measures to prevent the failure of the technical supply facilities required for the operation of system components with which information from cloud customers is processed, are documented and set up in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) with respect to the following aspects:
a) Operational redundancy (N+1) in power and cooling supply
b) Use of appropriately sized uninterruptible power supplies (UPS) and emergency power systems (NEA), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPS and NEA is checked at least annually by suitable tests and exercises (cf. BCM-04 – Verification, updating and testing of business continuity).
c) Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations.
d) Protection of power supply and telecommunications lines against interruption, interference, damage and eavesdropping. The protection is checked regularly, but at least every two years, as well as in case of suspected manipulation by qualified personnel regarding the following aspects:
• Traces of violent attempts to open closed distributors;
• Up-to-datedness of the documentation in the distribution list;
• Conformity of the actual wiring and patching with the documentation;
• The short-circuits and earthing of unneeded cables are intact; and
• Impermissible installations and modifications.

bernard@bornaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
BigQuery Omni is hosted on third-party infrastructure, and protection against interruptions caused by power failures and related risks is the responsibility of the subservice organizations.	Not applicable.	Not applicable.
Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s). A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No data centers that used river water for cooling were selected for testing during the period.	Observed generators on-site and during the facility capabilities presentation for a sample of data centers to determine that redundant power and cooling systems were equipped to support the continued operation of critical data center equipment in the event of a primary power source failure.	No exceptions noted.
	Inspected documentation of site UPS system duration at full capacity and generator start-up times for a sample of data centers to determine that UPS and Emergency Power Supplies (EPS) were designed to meet the Service Level Agreement (SLA) availability requirements.	No exceptions noted.
	Inquired of management and inspected documentation for data center facilities to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether any facility selected for testing that used river water for cooling maintained prerequisite water levels, air temperature, and water temperatures necessary for air conditioning.	Not tested. No data centers that used river water for cooling were selected for testing during the period.

bernard@pomeker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Power management and distribution systems are utilized to protect critical data center equipment from disruption or damage.	Inspected the organization's data center security requirements and calculated generator fuel burn rates for a sample of data centers to determine that power management and distribution systems protected critical equipment from disruption or damage and ensured at least 24 hours of operation with on-hand fuel in the event of an external power failure, as per security requirements and resupply contracts.	No exceptions noted.
Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.	Observed engineering documentation demonstrating UPS capabilities, generator start-up times, and cooling system redundancy for a sample of data centers to determine that redundant UPS and cooling systems were in place to protect critical equipment from disruption and damage.	No exceptions noted.
	Inspected internal audit documentation to determine that physical barriers were maintained to protect telecommunication lines against interruption, interference, damage, and eavesdropping, with oversight by qualified personnel, at least every two years.	No exceptions noted.
Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Inspected documentation of data center security reviews performed for all in-scope data centers to determine that data center security measures were assessed at least annually and the results were reviewed by executive management.	No exceptions noted.

bernard@bornaker.ru

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	Inspected maintenance records for a sample of data centers to determine that critical equipment (generators, UPS systems, chillers, fire suppression systems, emergency lighting, and HVAC systems) were continuously monitored and maintained through routine inspections, regular maintenance, and ad-hoc repairs in accordance with organizational requirements.	No exceptions noted.
	Observed systems and personnel monitoring climate controls in sensitive data center zones and triggered alerts for a sample of data centers to determine that critical equipment supporting products and services was continuously monitored.	No exceptions noted.
PS-07: Surveillance of Operational and Environmental Parameters The operating parameters of the technical utilities (cf. PS-06) and the environmental parameters of the premises and buildings related to the cloud service provided are monitored and controlled in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). When the permitted control range is exceeded, the responsible departments of the Cloud-Provider are automatically informed in order to promptly initiate the necessary measures for return to the control range.		
BigQuery Omni is hosted on third-party infrastructure, and surveillance of operational and environmental parameters is the responsibility of the subservice organizations.	Not applicable.	Not applicable.
Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	Inspected maintenance records for a sample of data centers to determine that critical equipment (generators, UPS systems, chillers, fire suppression systems, emergency lighting, and HVAC systems) were continuously monitored and maintained through routine inspections, regular maintenance, and ad-hoc repairs in accordance with organizational requirements.	No exceptions noted.

bernard@rofimaker.io

5.5 Physical Security (PS): Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Observed systems and personnel monitoring climate controls in sensitive data center zones and triggered alerts for a sample of data centers to determine that critical equipment supporting products and services was continuously monitored.	No exceptions noted.
Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Inspected documentation of data center security reviews performed for all in-scope data centers to determine that data center security measures were assessed at least annually and the results were reviewed by executive management.	No exceptions noted.

bernard@bunraker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OPS-01: Capacity Management – Planning The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks. The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload. Cloud Service Providers take appropriate measures to ensure that they continue to meet the requirements agreed with cloud customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources, in particular those relating to the dedicated use of system components, in accordance with the respective agreements.		
The organization makes procedures related to the management of information processing resources available. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	Inspected the organization's resource management documentation to determine that procedures related to managing information processing resources were made available and included guidance on requesting, monitoring, maintaining resources, and forecasting capacity requirements to identify usage trends and manage system overload.	No exceptions noted.
The organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	Inspected the annual planning index and timeline to determine that the organization managed the capacity of its information processing resources through planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
	Inspected the internal capacity monitoring dashboards and reviewed allocation reports and redundancy requirement metrics to determine that the organization managed the capacity of its information processing resources through planning, monitoring, and adjusting resources based on usage and system performance, integrating forecasts into SLA-compliant provisioning.	No exceptions noted.

bernard@ormako.no

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	No exceptions noted.
Google Cloud performs annual planning of resources which are determined based on company goals.	Inspected the organization's resource planning documentation to determine that Google Cloud performed an annual planning of resources, which were determined based on organizational goals.	No exceptions noted.
OPS-02: Capacity Management – Monitoring Technical and organizational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the Cloud Service Provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.		
The organization provides monitoring capabilities for customers of cloud services.	Inspected monitoring dashboards in the customer portal to determine that capacity and availability monitoring resources were provided in a self-service portal, allowing cloud service customers to control and monitor their system resources.	No exceptions noted.

bernard@brinker.in

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	Inspected the annual planning index and timeline to determine that the organization managed the capacity of its information processing resources through planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
	Inspected the internal capacity monitoring dashboards and reviewed allocation reports and redundancy requirement metrics to determine that the organization managed the capacity of its information processing resources through planning, monitoring, and adjusting resources based on usage and system performance, integrating forecasts into SLA-compliant provisioning.	No exceptions noted.
The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Inspected the Google Cloud Platform (GCP) ToS to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications such as the ToS.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications.	No exceptions noted.

bernard@bornaker.net

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization makes procedures related to the management of information processing resources available. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	Inspected the organization's resource management documentation to determine that procedures related to managing information processing resources were made available and included guidance on requesting, monitoring, maintaining resources, and forecasting capacity requirements to identify usage trends and manage system overload.	No exceptions noted.
OPS-03: Capacity Management – Controlling of Resources Depending on the capabilities of the respective service model, the cloud customer can control and monitor the allocation of the system resources assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.		
The organization provides monitoring capabilities for customers of cloud services.	Inspected monitoring dashboards in the customer portal to determine that capacity and availability monitoring resources were provided in a self-service portal, allowing cloud service customers to control and monitor their system resources.	No exceptions noted.
OPS-04: Protection Against Malware – Concept Policies and instructions that provide protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects: • Use of system-specific protection mechanisms; • Operating protection programs on system components under the responsibility of the Cloud Service Provider that are used to provide the cloud service in the production environment; and • Operation of protection programs for employees' terminal equipment.		

bernard@hotmaker.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has implemented mechanisms to protect its information assets against malicious activity (e.g. malware, spam, phishing).	Inspected Vulnerability Management and System Security Policies and Guidelines to determine that antivirus, antimalware, antispam, and antiphishing tools were implemented and that technical measures were in place to securely configure, monitor, and protect customer and Google cloud administration management consoles and information assets against malicious activity.	No exceptions noted.
	Inspected global policy configuration of antivirus, antimalware, and antispam tools on each in-scope operating system type to determine that mechanisms were implemented to protect information assets against malicious activity, with updates applied at the highest frequency offered contractually by vendors.	No exceptions noted.
Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Inspected administrative operations procedures for the organization's cloud computing environment on the external Quickstarts web page to determine that procedures were documented and made available to customers.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.

bernard@bertmaker.fr

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
OPS-05: Protection Against Malware – Implementation System components under the Cloud Service Provider's responsibility that are used to deploy the cloud service in the production environment are configured with malware protection according to the policies and instructions. If protection programs are set up with signature and behavior-based malware detection and removal, these protection programs are updated at least daily.		
The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and alerting configurations to determine that policies and protection mechanisms were documented and configured for detecting and reporting operational issues.	No exceptions noted.
	Inspected monitoring tool dashboards, alerting configurations, and an example alert to determine that monitoring tools were provided to personnel for detecting and reporting operational issues and that protection mechanisms were configured for automatic monitoring.	No exceptions noted.

bernard@crimekorin

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Integrity checks are in place at the file system level to ensure data integrity.	Inspected the file integrity monitoring dashboard, status reports, and scan configurations of the integrity assurance system for an example node to determine that integrity checks were implemented at the file system level to ensure data integrity.	No exceptions noted.
Deviations from predefined operating system (OS) configurations running on production machines are detected and corrected.	Inspected monitoring tool configurations to determine that deviations from predefined OS configurations on production machines were detected and corrected.	No exceptions noted.
The organization has implemented mechanisms to protect its information assets against malicious activity (e.g. malware, spam, phishing).	Inspected Vulnerability Management and System Security Policies and Guidelines to determine that antivirus, antimalware, antispam, and antiphishing tools were implemented and that technical measures were in place to securely configure, monitor, and protect customer and Google Cloud administration management consoles and information assets against malicious activity.	No exceptions noted.
	Inspected global policy configuration of antivirus, antimalware, and antispam tools on each in-scope operating system type to determine that mechanisms were implemented to protect information assets against malicious activity, with updates applied at the highest frequency offered contractually by vendors.	No exceptions noted.

bernard@bomtaker.in

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OPS-06: Data Backup and Recovery – Concept Policies and instructions for data backup and recovery are documented, communicated and provided in accordance with SP-01 regarding the following aspects. • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the art form; • Access to the backed-up data and the execution of restores is performed only by authorized persons; and • Tests of recovery procedures (cf. OPS-08).		
This criterion is not applicable to GCP. Rather than using traditional backup and recovery mechanisms, GCP addresses data redundancy through replication by writing data to multiple clusters within Cloud Regions.	Not applicable.	Not applicable.
OPS-07: Data Backup and Recovery – Monitoring The execution of data backups is monitored by technical and organizational measures. Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud customers or the Cloud Service Provider's business requirements regarding the scope and frequency of data backup and the duration of storage.		
This criterion is not applicable to GCP. Data redundancy is achieved through replication across multiple clusters within Cloud Regions, removing the need for traditional backup monitoring.	Not applicable.	Not applicable.
OPS-08: Data Backup and Recovery – Regular Testing Restore procedures are tested regularly, at least annually. The tests allow an assessment to be made as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02). Deviations from the specifications are reported to the responsible personnel or system components so that these can promptly assess the deviations and initiate the necessary actions.		

bernard@bolmaker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
This criterion is not applicable to GCP. Data redundancy is ensured through replication across multiple clusters within Cloud Regions, eliminating the need for traditional restore testing.	Not applicable.	Not applicable.
OPS-09: Data Backup and Recovery – Storage The Cloud Service Provider transfers data to be backed up to a remote location or transports these on backup media to a remote location. If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art. The distance to the main site is chosen after sufficient consideration of the factors recovery times and impact of disasters on both sites. The physical and environmental security measures at the remote site are at the same level as at the main site.		
BigQuery Omni is hosted on third-party infrastructure, and data backup and recovery are the responsibility of the subservice organizations.	Not applicable.	Not applicable.
The organization uses encryption to secure user data in transit between the organization's production facilities.	Inspected the organization's Cryptographic Guidelines to determine that encryption was required to secure user data in transit between production facilities.	No exceptions noted.
	Inspected encryption configuration files and required Transport Layer Security (TLS) protocols to determine that encryption was used to secure user data in transit between production facilities.	No exceptions noted.
The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the replication tool dashboard; monitoring tool dashboard; and filesystem, datastore, and network configurations for products and networks to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities.	No exceptions noted.

bernard@hotmaker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of customer data through the implementation of backups within the organization's information processing resources.	No exceptions noted.
Data center perimeters are defined and secured via physical barriers.	Observed structural features, including fenced perimeters, doors, walls, and segregated security zones, for a sample of data centers to determine that data center perimeters were defined by physical barriers.	No exceptions noted.
	Observed locks on doors, security personnel monitoring sensitive data center zones, and security system alerts to determine that data center perimeters were secured through physical security controls.	No exceptions noted.
OPS-10: Logging and Monitoring – Concept The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events on system components within its area of responsibility. These policies and instructions are documented, communicated and provided according to SP-01 with respect to the following aspects: • Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs; • Define roles and responsibilities for setting up and monitoring logging; • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.		

bernard@bunnaker.ru

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has established guidelines for governing the installation of software on organization-owned assets.	Inspected the Third-Party Software Installation Security Guidelines to determine that guidelines were established to govern software installation on organization-owned assets.	No exceptions noted.
Security event logs are protected, and access is restricted to authorized personnel.	Inspected the Security Logging Policy, security event log protection configuration, and the list of users with access to security event logs and their job titles to determine that security event logs were protected and access was restricted to authorized personnel.	No exceptions noted.
The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and alerting configurations to determine that policies and protection mechanisms were documented and configured for detecting and reporting operational issues.	No exceptions noted.
	Inspected monitoring tool dashboards, alerting configurations, and an example alert to determine that monitoring tools were provided to relevant personnel for detecting and reporting operational issues and that protection mechanisms were configured for automatic monitoring.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.

bernard@bountiker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
The organization has geographically dispersed personnel responsible for managing security incidents.	Inspected the security team intranet web page and schedule to determine that personnel were geographically dispersed to manage security incidents.	No exceptions noted.
OPS-11: Logging and Monitoring – Metadata Management Concept Policies and instructions for the secure handling of metadata (usage data) are documented, communicated and provided according to SP-01 with regard to the following aspects: • Metadata is collected and used solely for billing, incident management and security incident management purposes; • Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user; • No commercial use; • Storage for a fixed period reasonably related to the purposes of the collection; • Immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary; and • Provision to cloud customers according to contractual agreements		

bernard@bernaker.ch

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	Inspected the launch procedures and guidelines to determine that design documentation was required to be completed, reviewed, and approved before the release of a feature launch that introduced new collection, processing, or sharing of user data was released.	No exceptions noted.
	Inspected configurations enforcing required approvals and launch tickets for example launches to determine that design documentation was completed, reviewed, and approved before the release of a feature launch that introduced new collection, processing, or sharing of user data was released.	No exceptions noted.
Customers of the organization's services are provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.	Inspected the CDPA to determine that customers were provided with a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the service's functionality.	No exceptions noted.
	Observed the customer account interface in an example environment to determine that customers were provided with a mechanism within the service to access, correct, and erase Customer Data created by their accounts, consistent with the service's functionality.	No exceptions noted.
The organization has policies and guidelines in place which govern the use and protection of identifiable data.	Inspected the Data Security Policy and Data Categorization Guidelines to determine that policies and procedures governed the use and protection of identifiable data.	No exceptions noted.

bernard@bonnaker.fr

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Data Anonymization Policy to determine that policies and procedures required the anonymization of identifiable or pseudonymous production data before it was used in non-production environments.	No exceptions noted.
	Inspected tickets and review documentation for a sample of anonymization reviews to determine that anonymization of identifiable or pseudonymous production data was required before use in non-production environments.	No exceptions noted.
Where the organization is a data processor, the organization maintains the necessary records of processing in accordance with contractual obligations to controllers.	Inspected the Google Cloud Privacy Notice, internal guidelines, and Privacy Design Document (PDD) template, and metadata handling configurations to determine that the organization-maintained documentation and system configurations reflecting records of processing activities in accordance with contractual obligations to controllers.	No exceptions noted.
The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and alerting configurations to determine that policies and protection mechanisms were documented and configured for detecting and reporting operational issues.	No exceptions noted.

bernard@bornaker.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected monitoring tool dashboards, alerting configurations, and an example alert to determine that monitoring tools were provided to relevant personnel for detecting and reporting operational issues and that protection mechanisms were configured for automatic monitoring.	No exceptions noted.
The organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the CDPA, Data Security Policy, Security Classification Labeling Guidelines, and the Data Categorization Guidelines to determine that the organization had established policies and guidelines to define customer data and govern data classification, labeling, and security and that the organization's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and updated at least annually.	No exceptions noted.
	Inspected the documented safeguards in the Data Security Policy and the guidance provided to product teams on handling metadata to determine that the organization defined and implemented rules for the collection, access, processing, handling, retention, and deletion of metadata.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.

bernard@goldmaker.fr

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
OPS-12: Logging and Monitoring – Access, Storage and Deletion The requirements for the logging and monitoring of events and for the secure handling of metadata are implemented by technically supported procedures with regard to the following restrictions: • Access only for authorized users and systems; • Retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.		
At a minimum, security event logs must include the following: user ID, event type, timestamp, success/failure indication, event origination, and affected data/resource identifier. Security event logs are retained for a minimum of one (1) year.	Inspected log management tool configurations and example logs to determine that audit logs included, at a minimum, user ID, event type, timestamp, success or failure indication, event origination, and affected data or resource identifier and that logs were retained for at least one year.	No exceptions noted.

bernard@burnaker.ly

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Corporate Activity Retention Guidelines, log retention configurations, and example audit logs to determine that audit logs were retained for at least one year and that log data was deleted once it was no longer needed for its original purpose.	No exceptions noted.
The organization monitors its networks and systems for threats to information security.	Inspected the Security Logging Policy, log monitoring configurations, and incident response on-call schedule to determine that the organization monitored its networks and systems for information security threats.	No exceptions noted.
	Inspected job titles and organizational structures for a sample of personnel with logical access to audit logs to determine that access was restricted to authorized personnel.	No exceptions noted.
The organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the CDPA, Data Security Policy, Security Classification Labeling Guidelines, and the Data Categorization Guidelines to determine that the organization had established policies and guidelines to define customer data and govern data classification, labeling, and security and that the organization's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and updated at least annually.	No exceptions noted.

bernard@bonmaker.fr

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the documented safeguards in the Data Security Policy and the guidance provided to product teams on handling metadata to determine that the organization defined and implemented rules for the collection, access, processing, handling, retention, and deletion of metadata.	No exceptions noted.
The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with the data retention and deletion policy.	No exceptions noted.
	Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
Security event logs are protected, and access is restricted to authorized personnel.	Inspected the Security Logging Policy, security event log protection configuration, and the list of users with access to security event logs and their job titles to determine that security event logs were protected and access was restricted to authorized personnel.	No exceptions noted.
The organization has policies and guidelines in place which govern the use and protection of identifiable data.	Inspected the Data Security Policy and Data Categorization Guidelines to determine that policies and procedures governed the use and protection of identifiable data.	No exceptions noted.

bernard@boilmaker.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Data Anonymization Policy to determine that policies and procedures required the anonymization of identifiable or pseudonymous production data before it was used in non-production environments.	No exceptions noted.
	Inspected tickets and review documentation for a sample of anonymization reviews to determine that anonymization of identifiable or pseudonymous production data was required before use in non-production environments.	No exceptions noted.
OPS-13: Logging and Monitoring – Identification of Events The logging data is automatically monitored for events that may violate the protection goals in accordance with the logging and monitoring requirements. This also includes the detection of relationships between events (event correlation). Identified events are automatically reported to the appropriate departments for prompt evaluation and action.		
The organization has a dedicated team responsible for managing security & privacy incidents.	Inspected the security team's internal web page and schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.	No exceptions noted.
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these	No exceptions noted.

bernard@bornaker.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.
Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.

bernard@hotmaker.jo

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	No exceptions noted.
The organization maintains an up-to-date, accurate client device inventory.	Inspected the procedures for inventorying assets and an example of the client asset inventory review performed to determine that the organization maintained an updated, accurate, and consistent client device inventory throughout the asset lifecycle.	No exceptions noted.
OPS-14: Logging and Monitoring – Storage of the Logging Data The Cloud Service Provider retains the generated log data and keeps these in an appropriate, unchangeable and aggregated form, regardless of the source of such data, so that a central, authorized evaluation of the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected. Between logging servers and the assets to be logged, authentication takes place to protect the integrity and authenticity of the information transmitted and stored. The transfer takes place using state-of-the-art encryption or a dedicated administration network (out-of-band management).		
Customer data that is uploaded or created is encrypted at rest.	Inspected the organization's Cryptographic Policy and default encryption-at-rest web page to determine that customer data uploaded or created was required to be encrypted at rest according to storage-level encryption requirements.	No exceptions noted.
	Inspected data backup encryption configurations and encryption settings for storage devices containing customer data to determine that uploaded and created customer data was encrypted at rest.	No exceptions noted.

bernard@bottAker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Customer-Managed Encryption Keys guidance web page to determine that encryption keys could be controlled by the end user.	No exceptions noted.
At a minimum, security event logs must include the following: user ID, event type, timestamp, success/failure indication, event origination, and affected data/resource identifier. Security event logs are retained for a minimum of one (1) year.	Inspected log management tool configurations and example logs to determine that audit logs included, at a minimum, user ID, event type, timestamp, success or failure indication, event origination, and affected data or resource identifier and that logs were retained for at least one year.	No exceptions noted.
	Inspected the Corporate Activity Retention Guidelines, log retention configurations, and example audit logs to determine that audit logs were retained for at least one year and that log data was deleted once it was no longer needed for its original purpose.	No exceptions noted.
The organization uses encryption to secure user data in transit between the organization's production facilities.	Inspected the organization's Cryptographic Guidelines to determine that encryption was required to secure user data in transit between production facilities.	No exceptions noted.
	Inspected encryption configuration files and required TLS protocols to determine that encryption was used to secure user data in transit between production facilities.	No exceptions noted.
Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	Inspected the organization's Cryptographic Policy and the CDPA web page available to external users to determine that encryption mechanisms were required and communicated to protect user authentication and administrator sessions transmitted over the Internet.	No exceptions noted.

bernard@bothaker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected server scan results and encryption configurations and observed user administrator connection settings to determine that encryption mechanisms were used to protect user authentication and administrator sessions transmitted over the Internet.	No exceptions noted.
Security event logs are protected, and access is restricted to authorized personnel.	Inspected the Security Logging Policy, security event log protection configuration, and the list of users with access to security event logs and their job titles to determine that security event logs were protected and access was restricted to authorized personnel.	No exceptions noted.
The organization provides monitoring capabilities for customers of cloud services.	Inspected monitoring dashboards in the customer portal to determine that capacity and availability monitoring resources were provided in a self-service portal, allowing cloud service customers to control and monitor their system resources.	No exceptions noted.
OPS-15: Logging and Monitoring – Accountability The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident. Interfaces are available to conduct forensic analyses and perform backups of infrastructure components and their network communication.		
Audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts.	Inspected log monitoring dashboards, audit logging configurations, and an example log to determine that audit logs were retained for events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support log auditability for detecting potentially suspicious or malicious activities.	No exceptions noted.

bernard@bernaker.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected audit logging and monitoring tools at both tenant level and Google internal levels, along with a sample of audit logs, to determine that retained logs covered privileged user access activities, authorized access attempts, and unauthorized access attempts to support security incident investigation.	No exceptions noted.
Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	No exceptions noted.
The organization provides monitoring capabilities for customers of cloud services.	Inspected monitoring dashboards in the customer portal to determine that capacity and availability monitoring resources were provided in a self-service portal, allowing cloud service customers to control and monitor their system resources.	No exceptions noted.

bernard@bernaker.in

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OPS-16: Logging and Monitoring – Configuration Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility is restricted to authorized users. Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).		
Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	Inspected TLS protocol configurations and the enforcement of two-factor authentication (user ID with password, security key, and/or certificate) to determine that access to internal support tools was restricted to authorized personnel using approved credentials.	No exceptions noted.
	Inspected semi-annual critical access group membership review evidence, a sample of critical access group members, and their job titles to determine that access to internal support tools was restricted to authorized personnel using approved credentials.	No exceptions noted.
The organization monitors its networks and systems for threats to information security.	Inspected the Security Logging Policy, log monitoring configurations, and incident response on-call schedule to determine that the organization monitored its networks and systems for information security threats.	No exceptions noted.
	Inspected job titles and organizational structures for a sample of personnel with logical access to audit logs to determine that access was restricted to authorized personnel.	No exceptions noted.
Changes to the organization's systems are tested before being deployed.	Inspected testing notes within change request tickets for a sample of system changes to determine that changes to the organization's systems were tested prior to deployment.	No exceptions noted.

bernard@bonfaker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.
	Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.
Security event logs are protected, and access is restricted to authorized personnel.	Inspected the Security Logging Policy, security event log protection configuration, and the list of users with access to security event logs and their job titles to determine that security event logs were protected and access was restricted to authorized personnel.	No exceptions noted.

bernard@bunmakerit.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OPS-17: Logging and Monitoring – Availability of the Monitoring Software The Cloud Service Provider monitors the system components for logging and monitoring in its area of responsibility. Failures are automatically and promptly reported to the Cloud Service Provider's responsible departments so that these can assess the failures and take required action.		
The organization has established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.	Inspected the security team intranet web page and schedule to determine that a dedicated security team was established to engage in the security and privacy of customer data and manage security 24/7 worldwide.	No exceptions noted.
The organization maintains a framework that defines how to organize a response to security and privacy incidents.	Inspected internal incident response web pages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and privacy incidents.	No exceptions noted.
Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	No exceptions noted.

bernard@uptimaker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization provides external users with mechanisms to report security issues, incidents and concerns.	Inspected Google support documentation and external support resources to determine that the organization provided external users with mechanisms to report security issues, incidents, and concerns.	No exceptions noted.
Audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts.	Inspected log monitoring dashboards, audit logging configurations, and an example log to determine that audit logs were retained for events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support log auditability for detecting potentially suspicious or malicious activities.	No exceptions noted.
	Inspected audit logging and monitoring tools at both tenant level and Google internal levels, along with a sample of audit logs, to determine that retained logs covered privileged user access activities, authorized access attempts, and unauthorized access attempts to support security incident investigation.	No exceptions noted.
The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	Inspected the BIA, BC planning documentation, and the organization's ISO 27001 SoA to determine that requirements were established for business continuity measures that maintained the availability of the organization's production infrastructure and services.	No exceptions noted.
	Inspected Disaster Resiliency Testing documentation, including assigned roles, responsibilities, risks, and recovery objectives within the BC Plan, to determine that the organization implemented business continuity measures to maintain the availability of its production infrastructure and services.	No exceptions noted.

bernard@brinker.in

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected documented recovery activities in the DR Report to determine that recovery activities were outlined to maintain the availability of the organization's production infrastructure and services.	No exceptions noted.
OPS-18: Managing Vulnerabilities, Malfunctions and Errors – Concept Guidelines and instructions with technical and organizational measures are documented, communicated and provided in accordance with SP-01 to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These guidelines and instructions contain specifications regarding the following aspects: • Regular identification of vulnerabilities; • Assessment of the severity of identified vulnerabilities; • Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and • Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.		
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, Priority Guidelines, and the online register of known vulnerabilities to determine that the organization implemented a vulnerability management program, including third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring that remediation plans were developed and implemented for all critical and high-security deficiencies and tracked within internal tools, and that security patches were applied based on vulnerability severity and assigned CVSS scores.	No exceptions noted.

bernard@botmaker.ir

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected vulnerability scanning frequency configurations, example monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
	Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability planning meetings to determine that security teams met regularly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.

bernard@bornaker.ch

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
OPS-19: Managing Vulnerabilities, Malfunctions and Errors – Penetration Tests The Cloud Service Provider has penetration tests carried out by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to a documented test methodology and include the system components relevant to the provision of the cloud service in the area of responsibility of the Cloud Service Provider, which have been identified as such in a risk analysis. The Cloud Service Provider assesses the severity of the findings made in penetration tests according to defined criteria. For findings with medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, actions must be taken within defined time windows for prompt remediation or mitigation.		
Penetration tests are performed using a defined methodology and frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes.	Inspected the semi-annual and continuous penetration test results to determine that tests were performed at least every six months by independent external auditors, using a methodology and frequency aligned with compliance requirements and customer commitments.	No exceptions noted.
	Inspected remediation plans for vulnerabilities identified during the semi-annual and continuous penetration test to determine that corrective actions were taken in accordance with vulnerability management processes and that plans were developed and changes were implemented to address, at a minimum, all high and medium vulnerabilities.	No exceptions noted.

bernard@bottmaker.ch

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, Priority Guidelines, and the online register of known vulnerabilities to determine that the organization implemented a vulnerability management program, including third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring that remediation plans were developed and implemented for all critical and high-security deficiencies and tracked within internal tools, and that security patches were applied based on vulnerability severity and assigned CVSS scores.	No exceptions noted.
	Inspected vulnerability scanning frequency configurations, example monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
	Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability planning meetings to determine that security teams met regularly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.

bernard@bornkerin

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
OPS-20: Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures The Cloud Service Provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness. Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness.		
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, Priority Guidelines, and the online register of known vulnerabilities to determine that the organization implemented a vulnerability management program, including third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring that remediation plans were developed and implemented for all critical and high-security deficiencies and tracked within internal tools, and that security patches were applied based on vulnerability severity and assigned CVSS scores.	No exceptions noted.
	Inspected vulnerability scanning frequency configurations, example monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
	Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.

bernard@hotmaker.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability planning meetings to determine that security teams met regularly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
The organization has a dedicated team responsible for managing security & privacy incidents.	Inspected the security team's internal web page and schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.	No exceptions noted.
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	No exceptions noted.
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.

bernard@bottaker.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.
OPS-21: Involvement of Cloud Customers in the Event of Incidents The Cloud Service Provider periodically informs the cloud customer on the status of incidents affecting the cloud customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements. As soon as an incident has been resolved from the Cloud Service Provider's perspective, the cloud customer is informed according to the contractual agreements, about the actions taken.		
The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	Inspected the Information Security and Privacy Incident Response Policy and the procedures for reporting an incident on the Company intranet to determine that the organization maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
	Inspected the requirement for timely notifications of data breaches to affected customers, in accordance with disclosure laws or contractual agreements, within the CDPA shared with customers to determine that the organization communicated policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.

bernard@boilmaker.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.
The organization provides external users with mechanisms to report security issues, incidents and concerns.	Inspected Google support documentation and external support resources to determine that the organization provided external users with mechanisms to report security issues, incidents, and concerns.	No exceptions noted.
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	No exceptions noted.

bernard@bothmer.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.
OPS-22: Testing and Documentation of Known Vulnerabilities System components in the area of responsibility of the Cloud Service Provider for the provision of the cloud service are automatically checked for known vulnerabilities at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18), the severity is assessed in accordance with defined criteria and measures for timely remediation or mitigation are initiated within defined time windows.		
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, Priority Guidelines, and the online register of known vulnerabilities to determine that the organization implemented a vulnerability management program, including third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring that remediation plans were developed and implemented for all critical and high-security deficiencies and tracked within internal tools, and that security patches were applied based on vulnerability severity and assigned CVSS scores.	No exceptions noted.

bernard@bunnaker.fr

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected vulnerability scanning frequency configurations, example monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
	Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability planning meetings to determine that security teams met regularly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
OPS-23: Managing Vulnerabilities, Malfunctions and Errors – System Hardening System components in the production environment used to provide the cloud service under the Cloud Service Provider's responsibility are hardened according to generally accepted industry standards. The hardening requirements for each system component are documented. If non-modifiable ("immutable") images are used, compliance with the hardening specifications as defined in the hardening requirements is checked upon creation of the images. Configuration and log files regarding the continuous availability of the images are retained.		
A standard image is utilized for the installation and maintenance of each production server.	Inspected the Change Management Policy, Source Code Guidelines, replication tool configurations, and automated compliance jobs to determine that a standard image was required, maintained, and periodically verified for production servers.	No exceptions noted.

bernard@bornaker.ch

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected monitoring tool configurations to determine that tools monitored production machines, detected deviations from predefined OS configurations, and applied corrections.	No exceptions noted.
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the network guidelines, production image enforcement tool configurations, customer image restriction cloud portal functionality, and default hardening standards for machines and containers to determine that virtual environments were hardened where the organization held a responsibility as outlined in the shared responsibilities and mechanisms were provided for restricting the selection of default hardened images for virtual machines and containers in the cloud environment.	No exceptions noted.
OPS-24: Separation of Datasets in the Cloud Infrastructure Cloud customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk analysis to ensure the confidentiality and integrity of this data.		
The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	Inspected the physical and logical network architecture, segmentation requirements, and network diagrams alongside the Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.

bernard@bbmaker.io

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected example network connection pathways within the network device monitoring tool and reviewed access control and authentication configurations to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.
The organization has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	Inspected documented logical and physical network diagrams to determine that the organization required mechanisms by default to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.
	Inspected web browser encryption settings for cloud services and the default system configuration settings within the cloud customer interface that enforced session timeouts to determine that the organization had implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.
Development, testing and build environments are separated from the production environment through the use of logical security controls.	Inspected the Security Design in Applications, Systems, and Services Policy and the Network Access Security Policy to determine that development, testing, and build environments were required to be separated from the production environment through the use of logical security controls.	No exceptions noted.

bernard@bothmakers.ro

5.6 Operations (OPS): Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected access control groups and the separate development, testing, build, and production environments within example project workflow configurations to determine that the development, testing, and build environments were separated from the production environment through the use of logical security controls.	No exceptions noted.
The organization has policies and guidelines in place which govern the use and protection of identifiable data.	Inspected the Data Security Policy and Data Categorization Guidelines to determine that policies and procedures governed the use and protection of identifiable data.	No exceptions noted.
	Inspected the Data Anonymization Policy to determine that policies and procedures required the anonymization of identifiable or pseudonymous production data before it was used in non-production environments.	No exceptions noted.
	Inspected tickets and review documentation for a sample of anonymization reviews to determine that anonymization of identifiable or pseudonymous production data was required before use in non-production environments.	No exceptions noted.

bernard@bernaker.in

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
IDM-01: Policy for User Accounts and Access Rights A role and rights concept based on the business and security requirements of the Cloud Service Provider as well as a policy for managing user accounts and access rights for internal and external employees of the Cloud Service Provider and system components that have a role in automated authorization processes of the Cloud Service Provider are documented, communicated and made available according to SP-01: • Assignment of unique usernames; • Granting and modifying user accounts and access rights based on the "least-privilege principle" and the "need-to-know" principle; • Segregation of duties between operational and monitoring functions ("Segregation of Duties"); • Segregation of duties between managing, approving and assigning user accounts and access rights; • Approval by authorized individual(s) or system(s) for granting or modifying user accounts and access rights before data of the cloud customer or system components used to provision the cloud service can be accessed; • Regular review of assigned user accounts and access rights; • Blocking and removing access accounts in the event of inactivity; • Time-based or event-driven removal or adjustment of access rights in the event of changes to job responsibility; • Two-factor or multi-factor authentication for users with privileged access; and • Requirements for the approval and documentation of the management of user accounts and access rights.		
Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.	Inspected authentication configurations for remote access to the corporate network, production machines, network devices, and support tools to determine that access required a unique ID, password, and/or machine certificate.	No exceptions noted.
	Inspected network timeout configurations to determine that active certificates expired and network sessions were automatically timed out after 20 hours of inactivity.	No exceptions noted.
The organization has policies and guidelines that govern access to information systems.	Inspected the organization's access control policies to determine that policies and guidelines were established to govern access to information systems.	No exceptions noted.

hernan@bothmaker.ie

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege.	Inspected the Account Security Policy and the Identity and Access Management Policy to determine that access to information resources, including data and the systems that stored or processed data, was required to be authorized based on the principle of least privilege.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

IDM-02: Granting and Change of User Accounts and Access Rights

Specified procedures for granting and modifying user accounts and access rights for internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorization processes of the Cloud Service Provider ensure compliance with the role and rights concept as well as the policy for managing user accounts and access rights.

bernard@bunkerlab.io

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Customer access to storage is managed through the application. Unique user IDs are utilized to enforce access separation between customer accounts.	Inspected separate test customer accounts to determine that storage access was managed through the application and that unique user IDs enforced access separation between customer accounts.	No exceptions noted.
External system users are identified and authenticated via the Google Accounts or the BYOID authentication system before access is granted.	Inspected the configuration used to identify and authenticate external system users via Google Accounts or the Bring Your Own Identity (BYOID) authentication system to determine that users were identified and authenticated before being granted access to cloud services.	No exceptions noted.
	Inspected the customer account creation process to determine that external system users created their own passwords and were identified and authenticated via Google Accounts or the BYOID authentication system before accessing cloud services.	No exceptions noted.
The organization has mechanisms in place to prevent deactivated or deleted user accounts from being reassigned to new users.	Inspected the user account management processes and configurations, including remote deactivation, deletion, and locking capabilities, to determine that mechanisms were in place to prevent deactivated or deleted user accounts from being reassigned to new users.	No exceptions noted.
The organization separates duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	Inspected the Identity and Access Management Policy to determine that the organization separated duties by granting users access based on job responsibilities and least privilege by limiting access to only authorized users.	No exceptions noted.

bernard@hoinaker.ro

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Observed an attempt to access a privileged system outside the user's job responsibilities to determine that the organization's separation of duties and principle of least privilege successfully limited access to authorized users only.	No exceptions noted.
Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	Inspected access control lists and the configuration for group administrator approval requirements enforced by the access control system prior to provisioning user access to system components to determine that access to production machines, support tools, and network devices was managed via access control lists and that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
	Inspected the access control management tool history log, tool configuration, and examples of a new hire and transferred employee to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
Customers of the organization's services are provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.	Inspected the CDPA to determine that customers were provided with a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the service's functionality.	No exceptions noted.
	Observed the customer account interface in an example environment to determine that customers were provided with a mechanism within the service to access, correct, and erase Customer Data created by their accounts, consistent with the service's functionality.	No exceptions noted.

bernard@brinker.io

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
IDM-03: Locking and Withdrawal of User Accounts in the Event of Inactivity or Multiple Failed Logins User accounts of internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorization processes of the Cloud Service Provider are automatically locked if they have not been used for a period of two months. Approval from authorized personnel or system components are required to unlock these accounts. Locked user accounts are automatically revoked after six months. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.		
The organization has an established policy specifying the use of emergency credentials.	Inspected the Emergency Access Credential Policy to determine that the organization established a policy specifying requirements for the use of emergency credentials.	No exceptions noted.
	Inspected emergency credential expiration configurations and a sample of checkout tickets to determine that credentials required approval from authorized personnel prior to checkout and expired 90 days after issuance.	No exceptions noted.
Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Inspected the critical access groups' configuration to determine that reviews were assigned to authorized group administrators, ensuring that logical access was restricted to authorized personnel and periodically reviewed.	No exceptions noted.
	Inspected a sample of semi-annual user membership reviews for critical access groups, performed by group administrators, to determine that access was appropriately restricted and all review activities were tracked to completion.	No exceptions noted.

bernard@batmaker.io

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected automatic account revocation configurations to determine that inappropriate access identified during the semi-annual critical access group membership reviews was removed at least hourly.	No exceptions noted.
Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.	Inspected authentication configurations for remote access to the corporate network, production machines, network devices, and support tools to determine that access required a unique ID, password, and/or machine certificate.	No exceptions noted.
	Inspected network timeout configurations to determine that active certificates expired and network sessions were automatically timed out after 20 hours of inactivity.	No exceptions noted.
IDM-04: Withdraw or Adjust Access Rights as the Task Area Changes Access rights are promptly revoked if the job responsibilities of the Cloud Service Provider's internal or external staff or the tasks of system components involved in the Cloud Service Provider's automated authorization processes change. Privileged access rights are adjusted or revoked within 48 hours after the change takes effect. All other access rights are adjusted or revoked within 14 days. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.		
Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis upon submission of a termination request by Human Resources or a manager.	Inspected the Identity and Access Management Policy to determine that the organization documented procedures for terminating user access to production machines, support tools, network devices, and corporate assets.	No exceptions noted.
	Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets to determine that access was automatically removed in a timely manner upon submission of a termination request by Human Resources or a manager.	No exceptions noted.

bernard@hotmoker.io

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the historical account activity log and access removal evidence for an example terminated user to determine that access to production machines, support tools, network devices, and corporate assets was automatically removed in a timely manner using the automated tool upon submission of a termination request.	No exceptions noted.
The organization maintains formal user registration and de-registration procedures for granting and revoking access.	Inspected the organization's access control policies to determine that formal user registration and deregistration procedures were maintained for granting and revoking access.	No exceptions noted.
Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	Inspected access control lists and the configuration for group administrator approval requirements enforced by the access control system prior to provisioning user access to system components to determine that access to production machines, support tools, and network devices was managed via access control lists and that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
	Inspected the access control management tool history log, tool configuration, and examples of a new hire and transferred employee to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.

bernard@bolimaker.fr

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
IDM-05: Regular Review of Access Rights Access rights of internal and external employees of the Cloud Service Provider as well as of system components that play a role in automated authorization processes of the Cloud Service Provider are reviewed at least once a year to ensure that they still correspond to the actual area of use. The review is carried out by authorized persons from the Cloud Service Provider's organizational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the employees or system components. Identified deviations will be dealt with promptly, but no later than 7 days after their detection, by appropriate modification or withdrawal of the access rights.		
Logical access to network devices is restricted to authorized personnel and is periodically reviewed.	Inspected critical access group code configuration assigning reviews to authorized group administrators to determine that logical access to network devices was restricted to authorized personnel and was reviewed semi-annually.	No exceptions noted.
	Inspected critical access group user membership reviews performed by group administrators for a sample of users with logical access to network devices to determine that critical access group memberships were reviewed semi-annually to ensure that access was restricted appropriately and that reviews were tracked to completion.	No exceptions noted.
Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Inspected the critical access groups' configuration to determine that reviews were assigned to authorized group administrators, ensuring that logical access was restricted to authorized personnel and periodically reviewed.	No exceptions noted.

bernard@hotmaker.jp

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected a sample of semi-annual user membership reviews for critical access groups, performed by group administrators, to determine that access was appropriately restricted and all review activities were tracked to completion.	No exceptions noted.
	Inspected automatic account revocation configurations to determine that inappropriate access identified during the semi-annual critical access group membership reviews was removed at least hourly.	No exceptions noted.
IDM-06: Privileged Access Rights Privileged access rights for internal and external employees as well as technical users of the Cloud Service Provider are assigned and changed in accordance to the policy for managing user accounts and access rights (cf. IDM-01) or a separate specific policy. Privileged access rights are personalized, limited in time according to a risk assessment and assigned as necessary for the execution of tasks ("need-to-know principle"). Technical users are assigned to internal or external employees of the Cloud Service Provider. Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases. The logged information is automatically monitored for defined events that may indicate misuse. When such an event is identified, the responsible personnel are automatically informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken in accordance with HR-04.		
Personnel access to sensitive internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	Inspected the Account Authentication Guidelines to determine that personnel access to sensitive internal systems and applications required two-factor authentication using a distinct user ID, password, and a security key or certificate.	No exceptions noted.

bernard@bornaker.ru

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the code enforcing user authentication prior to certificate issuance to determine that personnel access to sensitive internal systems and applications required two-factor authentication with a distinct user ID, password, and security key or certificate and that certificates were generated only after successful two-factor authentication for single sign-on.	No exceptions noted.
Only users with a valid user certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	Inspected the code enforcing user authentication prior to granting private key access to determine that only users with a valid user certificate, corresponding private key, and host-specific authorization could access production machines via Secure Shell (SSH).	No exceptions noted.
	Inspected the configuration enforcing key-based authentication to determine that SSH access to production machines was restricted to authorized users with valid digital certificates.	No exceptions noted.
The organization separates duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	Inspected the Identity and Access Management Policy to determine that the organization separated duties by granting users access based on job responsibilities and least privilege by limiting access to only authorized users.	No exceptions noted.
	Observed an attempt to access a privileged system outside the user's job responsibilities to determine that the organization's separation of duties and principle of least privilege successfully limited access to authorized users only.	No exceptions noted.

bernard@bbmaker.fr

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts.	Inspected log monitoring dashboards, audit logging configurations, and an example log to determine that audit logs were retained for events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support log auditability for detecting potentially suspicious or malicious activities.	No exceptions noted.
	Inspected audit logging and monitoring tools at both tenant level and Google internal levels, along with a sample of audit logs, to determine that retained logs covered privileged user access activities, authorized access attempts, and unauthorized access attempts to support security incident investigation.	No exceptions noted.
The organization has an established policy specifying the use of emergency credentials.	Inspected the Emergency Access Credential Policy to determine that the organization established a policy specifying requirements for the use of emergency credentials.	No exceptions noted.
	Inspected emergency credential expiration configurations and a sample of checkout tickets to determine that credentials required approval from authorized personnel prior to checkout and expired 90 days after issuance.	No exceptions noted.
The organization monitors its networks and systems for threats to information security.	Inspected the Security Logging Policy, log monitoring configurations, and incident response on-call schedule to determine that the organization monitored its networks and systems for information security threats.	No exceptions noted.

bernard@bonnaker.ro

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected job titles and organizational structures for a sample of personnel with logical access to audit logs to determine that access was restricted to authorized personnel.	No exceptions noted.
Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Inspected the critical access groups' configuration to determine that reviews were assigned to authorized group administrators, ensuring that logical access was restricted to authorized personnel and periodically reviewed.	No exceptions noted.
	Inspected a sample of semi-annual user membership reviews for critical access groups, performed by group administrators, to determine that access was appropriately restricted and all review activities were tracked to completion.	No exceptions noted.
	Inspected automatic account revocation configurations to determine that inappropriate access identified during the semi-annual critical access group membership reviews was removed at least hourly.	No exceptions noted.
Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	Inspected TLS protocol configurations and the enforcement of two-factor authentication (user ID with password, security key, and/or certificate) to determine that access to internal support tools was restricted to authorized personnel using approved credentials.	No exceptions noted.

bernard@bolmaker.io

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected semi-annual critical access group membership review evidence, a sample of critical access group members, and their job titles to determine that access to internal support tools was restricted to authorized personnel using approved credentials.	No exceptions noted.
Logical access to network devices is restricted to authorized personnel and is periodically reviewed.	Inspected critical access group code configuration assigning reviews to authorized group administrators to determine that logical access to network devices was restricted to authorized personnel and was reviewed semi-annually.	No exceptions noted.
	Inspected critical access group user membership reviews performed by group administrators for a sample of users with logical access to network devices to determine that critical access group memberships were reviewed semi-annually to ensure that access was restricted appropriately and that reviews were tracked to completion.	No exceptions noted.
IDM-07: Access to Cloud Customer Data The cloud customer is informed by the Cloud Service Provider whenever internal or external employees of the Cloud Service Provider read or write to the cloud customer's data processed, stored or transmitted in the cloud service or have accessed it without the prior consent of the cloud customer. The Information is provided whenever data of the cloud customer is/was not encrypted, the encryption is/was disabled for access or the contractual agreements do not explicitly exclude such information. The information contains the cause, time, duration, type and scope of the access. The information is sufficiently detailed to enable subject matter experts of the cloud customer to assess the risks of the access. The information is provided in accordance with the contractual agreements, or within 72 hours after the access.		

bernard@bornaker.fr

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization only processes user data in accordance with the applicable data processing terms and does not process user data for any other purpose.	Inspected the CDPA and log data access policies to determine that user data was processed only in accordance with applicable data processing terms, access to customer data required documented reasons and logging, and customer consent was given prior to access if data was not encrypted or encryption was disabled, unless excluded by contractual agreements.	No exceptions noted.
	Inspected the Data Access Policy and example access logs to determine that the organization only processed user data in accordance with the applicable data processing terms and not for any other purpose and that access to customer data required a documented reason and resulted in the creation of an access log.	No exceptions noted.
	Inspected the Data Access Policy and example access logs to determine that access to customer data required a documented reason and resulted in the creation of an access log.	No exceptions noted.
The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	Inspected the Information Security and Privacy Incident Response Policy and the procedures for reporting an incident on the Company intranet to determine that the organization maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.

bernard@bolmaker.fr

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the requirement for timely notifications of data breaches to affected customers, in accordance with disclosure laws or contractual agreements, within the CDPA shared with customers to determine that the organization communicated policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
IDM-08: Confidentiality of Authentication Information The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud provider and system components that are involved in automated authorisation processes of the cloud provider is done in an orderly manner that ensures the confidentiality of the information. If passwords are used as authentication information, their confidentiality is ensured by the following procedures, as far as technically possible: • Users can initially create the password themselves or must change an initial password when logging on to the system component for the first time. An initial password loses its validity after a maximum of 14 days. • When creating passwords, compliance with the password specifications (cf. IDM-09) is enforced as far as technically possible. • The user is informed about changing or resetting the password. • The server-side storage takes place using cryptographically strong hash functions. Deviations are evaluated by means of a risk analysis and mitigating measures derived from this are implemented.		
The organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Guidelines for Google Passwords document to determine that formal guidelines for passwords were established to govern the management and use of authentication mechanisms.	No exceptions noted.

bernard@hotmaker.ir

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected SSH idle time configurations on servers to determine that they were configured to enforce password requirements according to formal authentication guidelines.	No exceptions noted.
	Inspected corporate endpoint configurations to determine that users were locked out after a maximum of 15 minutes of inactivity in accordance with formal guidelines for managing authentication mechanisms.	No exceptions noted.
	Inspected the authentication configurations to determine that passwords were transmitted and stored using encrypted procedures according to formal password management guidelines.	No exceptions noted.
The organization has a password change system that enforces its password guidelines.	Inspected the Guidelines for Google Passwords document and performed a password change to determine that the password change system enforced guidelines as defined in relevant security policies.	No exceptions noted.
	Observed a user attempt to change their password without meeting requirements to determine that an error message was displayed and the password change was unsuccessful.	No exceptions noted.
Customer data that is uploaded or created is encrypted at rest.	Inspected the organization's Cryptographic Policy and default encryption-at-rest web page to determine that customer data uploaded or created was required to be encrypted at rest according to storage-level encryption requirements.	No exceptions noted.

bernard@bottmaker.io

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected data backup encryption configurations and encryption settings for storage devices containing customer data to determine that uploaded and created customer data was encrypted at rest.	No exceptions noted.
	Inspected the Customer-Managed Encryption Keys guidance web page to determine that encryption keys could be controlled by the end user.	No exceptions noted.
Personnel access to sensitive internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	Inspected the Account Authentication Guidelines to determine that personnel access to sensitive internal systems and applications required two-factor authentication using a distinct user ID, password, and a security key or certificate.	No exceptions noted.
	Inspected the code enforcing user authentication prior to certificate issuance to determine that personnel access to sensitive internal systems and applications required two-factor authentication with a distinct user ID, password, and security key or certificate and that certificates were generated only after successful two-factor authentication for single sign-on.	No exceptions noted.
The organization separates duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	Inspected the Identity and Access Management Policy to determine that the organization separated duties by granting users access based on job responsibilities and least privilege by limiting access to only authorized users.	No exceptions noted.

bernard@purmarker.nl

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Observed an attempt to access a privileged system outside the user's job responsibilities to determine that the organization's separation of duties and principle of least privilege successfully limited access to authorized users only.	No exceptions noted.
The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected the confidentiality agreement template to determine that the organization had established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
	Inspected confidentiality agreement acknowledgements for a sample of extended workforce personnel to determine that extended workforce personnel acknowledged the organization's established confidentiality agreements, which defined responsibilities and expected behavior for the protection of information.	No exceptions noted.
The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inspected employee responsibilities and expected behavior for the protection of information within the confidentiality agreement template and Code of Conduct to determine that the organization established confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information.	No exceptions noted.

bernard@bornaker.ir

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected confidentiality agreement acknowledgements for a sample of employees to determine that employees acknowledged the organization's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information upon employment.	No exceptions noted.
IDM-09: Authentication Mechanisms System components in the Cloud Service Provider's area of responsibility that are used to provide the cloud service, authenticate users of the Cloud Service Provider's internal and external employees as well as system components that are involved in the Cloud Service Provider's automated authorization processes. Access to the production environment requires two-factor or multi-factor authentication. Within the production environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the Guideline for Key Management (cf. CRY-01). The password requirements are derived from a risk assessment and documented, communicated and provided in a password policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible.		
Remote access to corporate machines requires a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate.	Inspected the organization's Certificate Authority Policy and the Account Authentication Guidelines to determine that remote access to corporate machines required a digital certificate issued by the organization on the connecting device, as well as two-factor authentication in the form of user ID, password, security key, and/or certificate.	No exceptions noted.
	Inspected authentication configurations for remote access to corporate machines to determine that a digital certificate issued by the organization installed on the connecting device, along with two-factor authentication (user ID, password, security key, and/or certificate), was required for remote access.	No exceptions noted.

hernavi@bolmaker.ro

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.	Inspected the authentication configuration enforcing user IDs, passwords, security keys, and/or valid certificates to determine that logical access to organization-owned network devices was authenticated through enforced methods.	No exceptions noted.
Personnel access to sensitive internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	Inspected the Account Authentication Guidelines to determine that personnel access to sensitive internal systems and applications required two-factor authentication using a distinct user ID, password, and a security key or certificate.	No exceptions noted.
	Inspected the code enforcing user authentication prior to certificate issuance to determine that personnel access to sensitive internal systems and applications required two-factor authentication with a distinct user ID, password, and security key or certificate and that certificates were generated only after successful two-factor authentication for single sign-on.	No exceptions noted.
The organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Guidelines for Google Passwords document to determine that formal guidelines for passwords were established to govern the management and use of authentication mechanisms.	No exceptions noted.
	Inspected SSH idle time configurations on servers to determine that they were configured to enforce password requirements according to formal authentication guidelines.	No exceptions noted.

bernard@bpmaker.nl

5.7 Identity and Access Management (IDM): Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected corporate endpoint configurations to determine that users were locked out after a maximum of 15 minutes of inactivity in accordance with formal guidelines for managing authentication mechanisms.	No exceptions noted.
	Inspected the authentication configurations to determine that passwords were transmitted and stored using encrypted procedures according to formal password management guidelines.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@bonnaker.id

5.8 Cryptography and Key Management (CRY): Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
CRY-01: Policy for the Use of Encryption Procedures and Key Management Policies and instructions with technical and organizational safeguards for encryption procedures and key management are documented, communicated and provided according to SP-01, in which the following aspects are described: • Usage of strong encryption procedures and secure network protocols that correspond to the state-of-the-art; • Risk-based provisions for the use of encryption which are aligned with the data classification schemes (cf. AM-06) and consider the communication channel, type, strength and quality of the encryption; • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; and • Consideration of relevant legal and regulatory obligations and requirements.		
The organization maintains policies that define the requirements for the use of cryptography.	Inspected the organization's Cryptographic Policy and Account Authentication Guidelines to determine that policies were in place defining cryptography requirements.	No exceptions noted.
The organization prohibits the use of removable media for the storage of PII and SPII unless the data has been encrypted.	Inspected the Removable Media Security Policy, Data Security Policy, and Cryptographic Policy to determine that the use of removable media for storing Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) was prohibited unless the data was encrypted.	No exceptions noted.
The organization has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the Cryptographic Policy and Key Management Policy to determine that an established key management process was in place to support the organization's use of cryptographic techniques.	No exceptions noted.
	Inspected the code configuration for enforcing encryption, certificate authentication, and revocation to determine that an established key management process supported the organization's use of cryptographic techniques.	No exceptions noted.

bernard@trimaker.io

5.8 Cryptography and Key Management (CRY): Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
CRY-02: Encryption of Data for Transmission (Transport Encryption) The Cloud Service Provider has established procedures and technical measures for strong encryption and authentication for the transmission of data of cloud customers over public networks.		
The organization has established guidelines for protecting against the risks of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems.	Inspected the organization's remote access documentation to determine that guidelines were in place for protecting against teleworking risks and requiring encrypted communication systems for system access from remote locations.	No exceptions noted.

bernard@bornAker.fr

5.8 Cryptography and Key Management (CRY): Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the encryption configuration for remote authentication to determine that users accessed the system exclusively through encrypted communication systems.	No exceptions noted.
The organization uses encryption protocols to secure user data in transit between users and the organization's production facilities.	Inspected the organization's cryptographic documentation to determine that encryption protocols were required to secure user data in transit between users and production facilities.	No exceptions noted.
	Inspected the encryption configuration for all data in transit to determine that required encryption protocols secured user data between users and production facilities.	No exceptions noted.
	Inspected test server reports, website certificates, and GCP customer interface encryption protocols to determine that end-user traffic was encrypted in transit over public data-transmission networks.	No exceptions noted.
Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	Inspected the organization's Cryptographic Policy and the CDPA web page available to external users to determine that encryption mechanisms were required and communicated to protect user authentication and administrator sessions transmitted over the Internet.	No exceptions noted.

CRY-03: Encryption of Sensitive Data for Storage

The Cloud Service Provider has established procedures and technical safeguards to encrypt cloud customers' data during storage. The private keys used for encryption are known only to the cloud customer in accordance with applicable legal and regulatory obligations and requirements. Exceptions follow a specified procedure. The procedures for the use of private keys, including any exceptions, must be contractually agreed with the cloud customer.

bernard@bombaker.io

5.8 Cryptography and Key Management (CRY): Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization maintains policies that define the requirements for the use of cryptography.	Inspected the organization's Cryptographic Policy and Account Authentication Guidelines to determine that policies were in place defining cryptography requirements.	No exceptions noted.
Customer data that is uploaded or created is encrypted at rest.	Inspected the organization's Cryptographic Policy and default encryption-at-rest web page to determine that customer data uploaded or created was required to be encrypted at rest according to storage-level encryption requirements.	No exceptions noted.
	Inspected data backup encryption configurations and encryption settings for storage devices containing customer data to determine that uploaded and created customer data was encrypted at rest.	No exceptions noted.
	Inspected the Customer-Managed Encryption Keys guidance web page to determine that encryption keys could be controlled by the end user.	No exceptions noted.
The organization has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the Cryptographic Policy and Key Management Policy to determine that an established key management process was in place to support the organization's use of cryptographic techniques.	No exceptions noted.
	Inspected the code configuration for enforcing encryption, certificate authentication, and revocation to determine that an established key management process supported the organization's use of cryptographic techniques.	No exceptions noted.

bernard@bornaker.io

5.8 Cryptography and Key Management (CRY): Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
CRY-04: Secure Key Management Procedures and technical safeguards for secure key management in the area of responsibility of the Cloud Service Provider include at least the following aspects: • Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys; • Secure storage of keys (separation of key management system from application and middleware level) including description of how authorized users get access; • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realized; Handling of compromised keys; • Withdrawal and deletion of keys; and • If pre-shared keys are used, the specific provisions relating to the safe use of this procedure are specified separately.		
The organization has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the Cryptographic Policy and Key Management Policy to determine that an established key management process was in place to support the organization's use of cryptographic techniques.	No exceptions noted.
	Inspected the code configuration for enforcing encryption, certificate authentication, and revocation to determine that an established key management process supported the organization's use of cryptographic techniques.	No exceptions noted.

bernard@botmaker.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
COS-01: Technical Safeguards Based on the results of a risk analysis carried out according to OIS-06, the Cloud Service Provider has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns and/ or Distributed Denial of Service (DDoS) attacks. Data from corresponding technical protection measures implemented is fed into a comprehensive SIEM (Security Information and Event Management) system, so that (counter) measures regarding correlating events can be initiated. The safeguards are documented, communicated and provided in accordance with SP-01.		
Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Inspected the Security and Privacy Incident Response Policy, Security Logging Policy, and Device Configuration Guidelines to determine that monitoring tools were documented to send automated alerts to operational personnel based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.
	Inspected alert configurations and an example alert sent from monitoring tools to operational personnel to determine that automated alerts were sent based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.
The organization has implemented mechanisms to protect the production environment from denial-of-service attacks.	Inspected Denial of Service (DoS) protection documentation and escalation playbooks to determine that mechanisms were in place to protect the production environment against various DoS attacks.	No exceptions noted.
	Inspected DoS thresholds, alerting configurations, and an example DoS alert in the monitoring dashboard to determine that effective mechanisms protected the production environment against various DoS attacks.	No exceptions noted.

bernard@bitnaker.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Mechanisms are in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	Inspected firewall and network configurations, and an example alert, to determine that mechanisms detected and prevented unauthorized devices from connecting to the organization's network.	No exceptions noted.
The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	Inspected the security team intranet web page and schedule to determine that dedicated teams were established to monitor, maintain, manage, and secure the network.	No exceptions noted.
Network traffic is monitored through a combination of automated and manual controls and processes to detect anomalous network events which could indicate potential malicious activity.	Inspected diagrams, dashboards, and an example alert to determine that network traffic was monitored through automated and manual controls to detect anomalous events that could indicate malicious activity.	No exceptions noted.
Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	No exceptions noted.

bernard@dutmaker.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
COS-02: Security Requirements for Connections in the Cloud Service Provider's Network Specific security requirements are designed, published and provided for establishing connections within the Cloud Service Provider's network. The security requirements define for the Cloud Service Provider's area of responsibility: • In which cases the security zones are to be separated and in which cases cloud customers are to be logically or physically segregated; • Which communication relationships and which network and application protocols are permitted in each case; • How the data traffic for administration and monitoring is segregated from each on network level; • Which internal, cross-location communication is permitted; and • Which cross-network communication is allowed.		

bernard@bohmaker.it

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization's network security policies and guidelines apply to both physical and virtual networks.	Inspected the Network and Computer Security Policy and Network Device Guidelines to determine that network security policies and guidelines applied to both physical and virtual networks.	No exceptions noted.
The organization maintains production network diagrams and uses support tools to manage and visualize networks.	Inspected the support tools and network diagrams to determine that production network diagrams were maintained and support tools were used to manage and visualize networks.	No exceptions noted.
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the network guidelines, production image enforcement tool configurations, customer image restriction cloud portal functionality, and default hardening standards for machines and containers to determine that virtual environments were hardened where the organization held a responsibility as outlined in the shared responsibilities and mechanisms were provided for restricting the selection of default hardened images for virtual machines and containers in the cloud environment.	No exceptions noted.
The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	Inspected the physical and logical network architecture, segmentation requirements, and network diagrams alongside the Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.

bernard@auditmaker.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected example network connection pathways within the network device monitoring tool and reviewed access control and authentication configurations to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.
COS-03: Monitoring of Connections in the Cloud Service Provider's Network A distinction is made between trusted and untrusted networks. Based on a risk assessment, these are separated into different security zones for internal and external network areas (and DMZ, if applicable). Physical and virtualized network environments are designed and configured to restrict and monitor the established connection to trusted or untrusted networks according to the defined security requirements. The entirety of the conception and configuration undertaken to monitor the connections mentioned is assessed in a risk-oriented manner, at least annually, with regard to the resulting security requirements. Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18). At specified intervals, the business justification for using all services, protocols, and ports is reviewed. The review also includes the justifications for compensatory measures for the use of protocols that are considered insecure.		
The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected policies, design documentation, network topology diagrams, and firewall and global router configurations to determine that perimeter devices were implemented to protect the corporate network from external attacks.	No exceptions noted.
Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Inspected the Security and Privacy Incident Response Policy, Security Logging Policy, and Device Configuration Guidelines to determine that monitoring tools were documented to send automated alerts to operational personnel based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.

bernard@otmaker.ro

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected alert configurations and an example alert sent from monitoring tools to operational personnel to determine that automated alerts were sent based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, Priority Guidelines, and the online register of known vulnerabilities to determine that the organization implemented a vulnerability management program, including third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring that remediation plans were developed and implemented for all critical and high-security deficiencies and tracked within internal tools, and that security patches were applied based on vulnerability severity and assigned CVSS scores.	No exceptions noted.
	Inspected vulnerability scanning frequency configurations, example monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
	Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.

bernard@drinker.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability planning meetings to determine that security teams met regularly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment periodically to identify and evaluate risks.	No exceptions noted.
	Inspected the risk assessment documentation to determine that the organization's risk assessment considered the operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
	Inspected the Identity and Access Management Policy and risk assessment documentation to determine that a risk assessment was documented and evaluated the following risk areas: • Administration of rights profiles, approval and assignment of access, and access authorizations • Development, testing, and release of changes • Operation of the system components	No exceptions noted.
	Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas: • Processing, storage, and transmission of data of cloud customers with different protection needs	No exceptions noted.

bernard@otmdr.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	• Occurrence of weak points and malfunctions in technical protective measures for separating shared resources • Attacks via access points, including interfaces accessible from public networks • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons • Dependencies on subservice organizations	
The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	Inspected the security team intranet web page and schedule to determine that dedicated teams were established to monitor, maintain, manage, and secure the network.	No exceptions noted.
The organization's network security policies and guidelines apply to both physical and virtual networks.	Inspected the Network and Computer Security Policy and Network Device Guidelines to determine that network security policies and guidelines applied to both physical and virtual networks.	No exceptions noted.
COS-04: Cross-Network Access Each network perimeter is controlled by security gateways. The system access authorization for cross-network access is based on a security assessment based on the requirements of the cloud customers.		
The organization has implemented mechanisms to protect the production environment from denial-of-service attacks.	Inspected DoS protection documentation and escalation playbooks to determine that mechanisms were in place to protect the production environment against various DoS attacks.	No exceptions noted.
	Inspected DoS thresholds, alerting configurations, and an example DoS alert in the monitoring dashboard to determine that effective mechanisms protected the production environment against various DoS attacks.	No exceptions noted.

bernard@hotmail.fr

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected policies, design documentation, network topology diagrams, and firewall and global router configurations to determine that perimeter devices were implemented to protect the corporate network from external attacks.	No exceptions noted.
Mechanisms are in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	Inspected firewall and network configurations, and an example alert, to determine that mechanisms detected and prevented unauthorized devices from connecting to the organization's network.	No exceptions noted.
COS-05: Networks for Administration There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication (cf. IDM-09). Networks used by the Cloud Service Provider to migrate or create virtual machines are also physically or logically separated from other networks.		
The organization maintains production network diagrams and uses support tools to manage and visualize networks.	Inspected the support tools and network diagrams to determine that production network diagrams were maintained and support tools were used to manage and visualize networks.	No exceptions noted.
The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	Inspected the physical and logical network architecture, segmentation requirements, and network diagrams alongside the Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.

bernard@bornAker.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected example network connection pathways within the network device monitoring tool and reviewed access control and authentication configurations to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.
Mechanisms are in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	Inspected firewall and network configurations, and an example alert, to determine that mechanisms detected and prevented unauthorized devices from connecting to the organization's network.	No exceptions noted.
COS-06: Segregation of Data Traffic in Jointly Used Network Environments Data traffic of cloud customers in jointly used network environments is segregated on network level according to a documented concept to ensure the confidentiality and integrity of the data transmitted.		
The organization has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	Inspected documented logical and physical network diagrams to determine that the organization required mechanisms by default to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.
	Inspected web browser encryption settings for cloud services and the default system configuration settings within the cloud customer interface that enforced session timeouts to determine that the organization had implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.

bernard@hotmaker.ro

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected policies, design documentation, network topology diagrams, and firewall and global router configurations to determine that perimeter devices were implemented to protect the corporate network from external attacks.	No exceptions noted.
The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	Inspected the physical and logical network architecture, segmentation requirements, and network diagrams alongside the Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.
	Inspected example network connection pathways within the network device monitoring tool and reviewed access control and authentication configurations to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.
Penetration tests are performed using a defined methodology and frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes.	Inspected the semi-annual and continuous penetration test results to determine that tests were performed at least every six months by independent external auditors, using a methodology and frequency aligned with compliance requirements and customer commitments.	No exceptions noted.

bernard@bombaker.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected remediation plans for vulnerabilities identified during the semi-annual and continuous penetration test to determine that corrective actions were taken in accordance with vulnerability management processes and that plans were developed and changes were implemented to address, at a minimum, all high and medium vulnerabilities.	No exceptions noted.
Mechanisms are in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	Inspected firewall and network configurations, and an example alert, to determine that mechanisms detected and prevented unauthorized devices from connecting to the organization's network.	No exceptions noted.
COS-07: Documentation of the Network Topology The documentation of the logical structure of the network used to provision or operate the Cloud Service, is traceable and up to date, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions in accordance with contractual obligations. The documentation shows how the subnets are allocated and how the network is zoned and segmented. In addition, the geographical locations in which the cloud customers' data is stored are indicated.		
The organization maintains production network diagrams and uses support tools to manage and visualize networks.	Inspected the support tools and network diagrams to determine that production network diagrams were maintained and support tools were used to manage and visualize networks.	No exceptions noted.
The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	Inspected the physical and logical network architecture, segmentation requirements, and network diagrams alongside the Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control	No exceptions noted.

bernard@bornmaker.fr

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	
	Inspected example network connection pathways within the network device monitoring tool and reviewed access control and authentication configurations to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.
COS-08: Policies for Data Transmission Policies and instructions with technical and organizational safeguards in order to protect the transmission of data against unauthorized interception, manipulation, copying, modification, redirection or destruction are documented, communicated and provided according to SP-01. The policies and instructions establish a reference to the classification of information (cf. AM-06).		
The organization maintains policies that define the requirements for the use of cryptography.	Inspected the organization's Cryptographic Policy and Account Authentication Guidelines to determine that policies were in place defining cryptography requirements.	No exceptions noted.
The organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the CDPA, Data Security Policy, Security Classification Labeling Guidelines, and the Data Categorization Guidelines to determine that the organization had established policies and guidelines to define customer data and govern data classification, labeling, and security and that the organization's approach to meeting relevant statutory, regulatory, and	No exceptions noted.

bernard@bormaker.io

5.9 Communication Security (COS): Ensure the protection of information in networks and the corresponding information processing systems.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	contractual requirements was defined, documented, and updated at least annually.	
	Inspected the documented safeguards in the Data Security Policy and the guidance provided to product teams on handling metadata to determine that the organization defined and implemented rules for the collection, access, processing, handling, retention, and deletion of metadata.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@hotmaker.io

5.10 Portability and Interoperability (PI): Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
PI-01: Documentation and Safety of Input and Output Interfaces The cloud service can be accessed by other cloud services or IT systems of cloud customers through documented inbound and outbound interfaces. Further, the interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. Communication takes place through standardized communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements. Communication over untrusted networks is encrypted according to CRY-02. The type and scope of the documentation on the interfaces is geared to the needs of the cloud customers' subject matter experts in order to enable the use of these interfaces. The information is maintained in such a way that it is applicable for the cloud service's version which is intended for productive use.		
The organization provides customers with information regarding default encryption methods used to protect user data. Additional applications of cryptographic protections are documented and shared through public sites.	Inspected the CDPA and the organization's Default Encryption at Rest web page to determine that information regarding default encryption methods used to protect customer data was provided to customers and additional applications of cryptographic protections were documented and shared through public sites.	No exceptions noted.
The organization publishes specification and reference documentation for APIs to ensure interoperability.	Inspected data export specification documentation and application programming interface (API) reference documentation made available on the organization's website to determine that the organization published specifications and reference documentation for APIs to help ensure interoperability.	No exceptions noted.
The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected policies, design documentation, network topology diagrams, and firewall and global router configurations to determine that perimeter devices were implemented to protect the corporate network from external attacks.	No exceptions noted.

bernard@cotmeleon.io

5.10 Portability and Interoperability (PI): Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization maintains production network diagrams and uses support tools to manage and visualize networks.	Inspected the support tools and network diagrams to determine that production network diagrams were maintained and support tools were used to manage and visualize networks.	No exceptions noted.
Mechanisms are in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	Inspected firewall and network configurations, and an example alert, to determine that mechanisms detected and prevented unauthorized devices from connecting to the organization's network.	No exceptions noted.
PI-02: Contractual Agreements for the Provision of Data In contractual agreements, the following aspects are defined with regard to the termination of the contractual relationship, insofar as these are applicable to the cloud service: • Type, scope and format of the data the Cloud Service Provider provides to the cloud customer; • Definition of the timeframe, within which the Cloud Service Provider makes the data available to the cloud customer; • Definition of the point in time as of which the Cloud Service Provider makes the data inaccessible to the cloud customer and deletes these; and • The cloud customers' responsibilities and obligations to cooperate for the provision of the data. The definitions are based on the needs of subject matter experts of potential customers who assess the suitability of the cloud service with regard to a dependency on the Cloud Service Provider as well as legal and regulatory requirements.		
The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Inspected the CDPA on the organization's public web page to determine that policies on the return, transfer, and disposal of user data were maintained and made available to customers.	No exceptions noted.
The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Inspected the Google Cloud Platform (GCP) ToS to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications such as the ToS.	No exceptions noted.

bernard@bothmaker.io

5.10 Portability and Interoperability (PI): Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected Google's CDPA to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications.	No exceptions noted.
The organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the CDPA, Data Security Policy, Security Classification Labeling Guidelines, and the Data Categorization Guidelines to determine that the organization had established policies and guidelines to define customer data and govern data classification, labeling, and security and that the organization's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and updated at least annually.	No exceptions noted.
	Inspected the documented safeguards in the Data Security Policy and the guidance provided to product teams on handling metadata to determine that the organization defined and implemented rules for the collection, access, processing, handling, retention, and deletion of metadata.	No exceptions noted.
The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with the data retention and deletion policy.	No exceptions noted.

bernard@bcmaker.io

5.10 Portability and Interoperability (PI): Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
The approach to meeting relevant statutory, regulatory, and contractual requirements is defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	Inspected the product launch process, the relevant Google Cloud ToS, and the internal cloud compliance website to determine that the organization's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	No exceptions noted.
PI-03: Secure Deletion of Data The Cloud Service Provider's procedures for deleting the cloud customers' data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02). The deletion includes data in the cloud customer's environment, metadata and data stored in the data backups. The deletion procedures prevent recovery by forensic means.		
The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Inspected the CDPA on the organization's public web page to determine that policies on the return, transfer, and disposal of user data were maintained and made available to customers.	No exceptions noted.
The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with the data retention and deletion policy.	No exceptions noted.

bernard@bunraker.fr

5.10 Portability and Interoperability (PI): Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.

bernard@botmaker.lt

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
DEV-01: Policies for the Development/Procurement of Information Systems Policies and instructions with technical and organizational measures for the secure development of the cloud service are documented, communicated and provided in accordance with SP-01. The policies and instructions contain guidelines for the entire life cycle of the cloud service and are based on recognized standards and methods with regard to the following aspects: • Security in Software Development (Requirements, Design, Implementation, Testing and Verification); • Security in software deployment (including continuous delivery); and • Security in operation (reaction to identified faults and vulnerabilities).		
The organization has policies and guidelines governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy, the Security Requirements for Outsourced Software Development Policy, and the Source Code Guidelines, to determine that the organization had established policies and guidelines governing the secure development lifecycle, including requirements for outsourced development.	No exceptions noted.
The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.
	Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.

bernard@bolmaker.io

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
The organization requires subprocessors to meet security and privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements or other data processing terms.	Inspected the SDPA to determine that the organization required subprocessors to meet security and privacy requirements for safeguarding customer and service data, which were enforced via the SDPA addendum to contractual agreements or other data processing terms.	No exceptions noted.

bernard@brinker.ru

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
DEV-02: Outsourcing of the Development In the case of outsourced development of the cloud service (or individual system components), specifications regarding the following aspects are contractually agreed between the Cloud Service Provider and the outsourced development contractor: • Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognized standards and methods; • Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and • Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities.		
The organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	Inspected the CDPA and the Google Cloud Marketplace PIPA to determine that the organization required external partners to meet security and privacy requirements for safeguarding user data, and that requirements were enforced via the PIPA.	No exceptions noted.
	Inspected the ISA and the SDPA for a sample of processors and sub-processors supporting in-scope systems to determine that the organization had implemented a contractual addendum with processors and sub-processors.	No exceptions noted.
	Inspected the termination clause for service issues related to vendors within an example IPA and an example SDPA to determine that it defined the security obligations that processors (including sub-processors) had to meet to satisfy the organization's obligations regarding customer data.	No exceptions noted.

bernard@...

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has policies and guidelines governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy, the Security Requirements for Outsourced Software Development Policy, and the Source Code Guidelines, to determine that the organization had established policies and guidelines governing the secure development lifecycle, including requirements for outsourced development.	No exceptions noted.
The organization requires subprocessors to meet security and privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements or other data processing terms.	Inspected the SDPA to determine that the organization required subprocessors to meet security and privacy requirements for safeguarding customer and service data, which were enforced via the SDPA addendum to contractual agreements or other data processing terms.	No exceptions noted.

DEV-03: Policies for Changes to Information Systems

Policies and instructions with technical and organizational safeguards for change management of system components of the cloud service within the scope of software deployment are documented, communicated and provided according to SP-01 with regard to the following aspects:
• Criteria for risk assessment, categorization and prioritization of changes and related requirements for the type and scope of testing to be performed, and necessary approvals for the development/implementation of the change and releases for deployment in the production environment by authorized personnel or system components;
• Requirements for the performance and documentation of tests;
• Requirements for segregation of duties during development, testing and release of changes;
• Requirements for the proper information of cloud customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements;
• Requirements for the documentation of changes in system, operational and user documentation; and
• Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.

bernard@bolmaker.ro

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Inspected the Change Management Security Policy and secure coding guidelines to determine that policies and guidelines for tracking, testing, approving, and validating changes, including security code reviews, were in place.	No exceptions noted.
Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	Inspected the launch procedures and guidelines to determine that design documentation was required to be completed, reviewed, and approved before the release of a feature launch that introduced new collection, processing, or sharing of user data was released.	No exceptions noted.
	Inspected configurations enforcing required approvals and launch tickets for example launches to determine that design documentation was completed, reviewed, and approved before the release of a feature launch that introduced new collection, processing, or sharing of user data was released.	No exceptions noted.
Changes to customer facing services that may affect confidentiality, processing integrity and/or availability are communicated to relevant personnel and impacted customers.	Inspected alert notifications and change ticket communication history for a sample of changes to customer-facing services to determine that relevant personnel were notified of changes that could have affected security, confidentiality, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker web page, and the customer-facing log of vulnerabilities to determine that impacted customers were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.

bernard@bountaker.ir

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
System changes are reviewed and approved by a separate technical resource before moving into production.	Inspected change request tickets for a sample of system changes to determine that system changes were documented, tested, reviewed, and approved by a separate technical resource before moving into production.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@bunkerlabs.net

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
DEV-04: Safety Training and Awareness Program Regarding Continuous Software Delivery and Associated Systems, Components or Tools The Cloud Service Provider provides a training program for regular, target group-oriented security training and awareness for internal and external employees on standards and methods of secure software development and provision as well as on how to use the tools used for this purpose. The program is regularly reviewed and updated with regard to the applicable policies and instructions, the assigned roles and responsibilities and the tools used.		
The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.	Inspected the privacy and information security training content on tools, standards, and methods of secure software development and provisioning to determine that the organization provided annual training programs for both internal and external employees, focusing on secure software development practices and tool usage.	No exceptions noted.
	Inspected the compliance monitoring tool dashboard used by management to track employees' completion rates for required privacy and information security awareness training, configurations for the automated training enrollment tool, and an example of an email notification for overdue training to determine that the organization had established a privacy and information security training program covering both quantitative and qualitative measurements and that relevant personnel met the annual training completion requirements.	No exceptions noted.
	Inspected the privacy and information security training program content to determine that the organization reviewed and updated training content at least annually, based on the results achieved through the privacy and information security awareness training program.	No exceptions noted.

bernard@bottmaker.io

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
DEV-05: Risk Assessment, Categorization and Prioritization of Changes In accordance with the applicable policies (cf. DEV-03), changes are subjected to a risk assessment with regard to potential effects on the system components concerned and are categorized and prioritized accordingly.		
The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Inspected the Change Management Security Policy and secure coding guidelines to determine that policies and guidelines for tracking, testing, approving, and validating changes, including security code reviews, were in place.	No exceptions noted.
System changes are reviewed and approved by a separate technical resource before moving into production.	Inspected change request tickets for a sample of system changes to determine that system changes were documented, tested, reviewed, and approved by a separate technical resource before moving into production.	No exceptions noted.
Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	Inspected the launch procedures and guidelines to determine that design documentation was required to be completed, reviewed, and approved before the release of a feature launch that introduced new collection, processing, or sharing of user data was released.	No exceptions noted.
	Inspected configurations enforcing required approvals and launch tickets for example launches to determine that design documentation was completed, reviewed, and approved before the release of a feature launch that introduced new collection, processing, or sharing of user data was released.	No exceptions noted.

bernard@laetmaker.io

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Changes to customer facing services that may affect confidentiality, processing integrity and/or availability are communicated to relevant personnel and impacted customers.	Inspected alert notifications and change ticket communication history for a sample of changes to customer-facing services to determine that relevant personnel were notified of changes that could have affected security, confidentiality, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker web page, and the customer-facing log of vulnerabilities to determine that impacted customers were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.
DEV-06: Testing Changes Changes to the cloud service are subject to appropriate testing during software development and deployment. The type and scope of the tests correspond to the risk assessment. The tests are carried out by appropriately qualified personnel of the Cloud Service Provider or by automated test procedures that comply with the state-of-the-art. Cloud customers are involved in the tests in accordance with the contractual requirements. The severity of the errors and vulnerabilities identified in the tests, which are relevant for the deployment decision, is determined according to defined criteria and actions for timely remediation or mitigation are initiated.		
The organization tests, validates, and documents changes to its services prior to deployment to production.	Inspected change tickets for a sample of changes to determine that changes to services were tested, validated, and documented prior to deployment to production.	No exceptions noted.
Changes to the organization's systems are tested before being deployed.	Inspected testing notes within change request tickets for a sample of system changes to determine that changes to the organization's systems were tested prior to deployment.	No exceptions noted.

howard@bothker.io

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
System changes are reviewed and approved by a separate technical resource before moving into production.	Inspected change request tickets for a sample of system changes to determine that system changes were documented, tested, reviewed, and approved by a separate technical resource before moving into production.	No exceptions noted.
DEV-07: Logging of Changes System components and tools for source code management and software deployment that are used to make changes to system components of the cloud service in the production environment are subject to a role and rights concept according to IDM-01 and authorization mechanisms. They must be configured in such a way that all changes are logged and can therefore be traced back to the individuals or system components executing them.		
The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.
	Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.

bernard@batmaker.fr

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.
The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Inspected the Change Management Security Policy and secure coding guidelines to determine that policies and guidelines for tracking, testing, approving, and validating changes, including security code reviews, were in place.	No exceptions noted.
DEV-08: Version Control Version control procedures are set up to track dependencies of individual changes and to restore affected system components back to their previous state as a result of errors or identified vulnerabilities.		
The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.
	Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.

bernard@bunnoker.nl

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.
The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Inspected the Change Management Security Policy and secure coding guidelines to determine that policies and guidelines for tracking, testing, approving, and validating changes, including security code reviews, were in place.	No exceptions noted.
DEV-09: Approvals for Provision in the Production Environment Authorized personnel or system components of the Cloud Service Provider approve changes to the cloud service based on defined criteria (e.g., test results and required approvals) before these are made available to the cloud customers in the production environment. Cloud customers are involved in the release according to contractual requirements.		
Changes to network configurations are reviewed and approved prior to deployment.	Inspected documented change request tickets for a sample of manual network configuration changes to determine that manual changes were reviewed and approved prior to deployment.	No exceptions noted.
	Inspected a documented change ticket for an example automated network configuration change deployed by an automated tool following a pre-configured and manually reviewed change to determine that changes were reviewed and approved prior to deployment.	No exceptions noted.

bernard@bornaker.ru

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected a change ticket for an example change made to the automated deployment tool to determine that network configurations deployed through automation were reviewed and approved prior to deployment.	No exceptions noted.
Changes to the organization's systems are tested before being deployed.	Inspected testing notes within change request tickets for a sample of system changes to determine that changes to the organization's systems were tested prior to deployment.	No exceptions noted.
System changes are reviewed and approved by a separate technical resource before moving into production.	Inspected change request tickets for a sample of system changes to determine that system changes were documented, tested, reviewed, and approved by a separate technical resource before moving into production.	No exceptions noted.
The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.
	Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.

leonard@hotmaker.ro

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.
DEV-10: Separation of Environments Production environments are physically or logically separated from test or development environments to prevent unauthorized access to cloud customer data, the spread of malware, or changes to system components. Data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality.		
Development, testing and build environments are separated from the production environment through the use of logical security controls.	Inspected the Security Design in Applications, Systems, and Services Policy and the Network Access Security Policy to determine that development, testing, and build environments were required to be separated from the production environment through the use of logical security controls.	No exceptions noted.
	Inspected access control groups and the separate development, testing, build, and production environments within example project workflow configurations to determine that the development, testing, and build environments were separated from the production environment through the use of logical security controls.	No exceptions noted.
The organization has policies and guidelines in place which govern the use and protection of identifiable data.	Inspected the Data Security Policy and Data Categorization Guidelines to determine that policies and procedures governed the use and protection of identifiable data.	No exceptions noted.

bernard@bottmaker.ru

5.11 Procurement, Development and Modification of Information Systems (DEV): Ensure information security in the development cycle of cloud service system components.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Data Anonymization Policy to determine that policies and procedures required the anonymization of identifiable or pseudonymous production data before it was used in non-production environments.	No exceptions noted.
	Inspected tickets and review documentation for a sample of anonymization reviews to determine that anonymization of identifiable or pseudonymous production data was required before use in non-production environments.	No exceptions noted.
The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	Inspected the physical and logical network architecture, segmentation requirements, and network diagrams alongside the Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.
	Inspected example network connection pathways within the network device monitoring tool and reviewed access control and authentication configurations to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage, ensuring networks were physically and/or logically separated via access control mechanisms, only approved use cases were allowed, and exceptions required additional review and approval.	No exceptions noted.

bernard@bornAker.ro

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
SSO-01: Policies and Instructions for Controlling and Monitoring Third Parties Policies and instructions for controlling and monitoring third parties (e.g., service providers or suppliers) whose services contribute to the provision of the cloud service are documented, communicated and provided in accordance with SP-01 with respect to the following aspects: • Requirements for the assessment of risks resulting from the procurement of third-party services; • Requirements for the classification of third parties based on the risk assessment by the Cloud Service Provider and the determination of whether the third party is a subcontractor (cf. Supplementary Information); • Information security requirements for the processing, storage or transmission of information by third parties based on recognized industry standards; • Information security awareness and training requirements for staff; • applicable legal and regulatory requirements; • Requirements for dealing with vulnerabilities, security incidents and malfunctions; • Specifications for the contractual agreement of these requirements; • Specifications for the monitoring of these requirements; and • Specifications for applying these requirements also to service providers used by the third-parties, insofar as the services provided by these service providers also contribute to the provision of the cloud service.		
The organization has policies and guidelines that govern third-party relationships.	Inspected the Google VSA Guidelines and vendor risk assessment documentation to determine that policies and procedures were developed to govern third-party relationships.	No exceptions noted.
	Inspected third-party information and documentation within the vendor directory to determine that processes were in place to govern third-party relationships.	No exceptions noted.
Cloud Subprocessor security and privacy risk is assessed via periodic assessment of subprocessor control environment.	Inspected the VSA Guidelines and documentation for a sample of cloud subprocessors to determine that annual assessments of security and privacy risks in subprocessor control environments were performed.	No exceptions noted.

bernard@botmaker.io

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Subprocessor performance is regularly assessed and monitored via periodic business reviews.	Inspected the Subprocessor Business Reports for a sample of subprocessors to determine that subprocessor performance was regularly assessed and monitored through business reviews.	No exceptions noted.
The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
	Inspected NDA acknowledgements for a sample of external parties to determine that the organization established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.
The organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	Inspected the CDPA and the Google Cloud Marketplace PIPA to determine that the organization required external partners to meet security and privacy requirements for safeguarding user data, and that requirements were enforced via the PIPA.	No exceptions noted.
	Inspected the ISA and the SDPA for a sample of processors and sub-processors supporting in-scope systems to determine that the organization had implemented a contractual addendum with processors and sub-processors.	No exceptions noted.

bernard@bonnaker.io

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the termination clause for service issues related to vendors within an example IPA and an example SDPA to determine that it defined the security obligations that processors (including sub-processors) had to meet to satisfy the organization's obligations regarding customer data.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@bunnaker.ru

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization requires subprocessors to meet security and privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements or other data processing terms.	Inspected the SDPA to determine that the organization required subprocessors to meet security and privacy requirements for safeguarding customer and service data, which were enforced via the SDPA addendum to contractual agreements or other data processing terms.	No exceptions noted.
SSO-02: Risk Assessment of Service Providers and Suppliers Service providers and suppliers of the Cloud Service Provider undergo a risk assessment in accordance with the policies and instructions for the control and monitoring of third parties prior to contributing to the delivery of the cloud service. The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the Cloud Service Provider during service usage. The risk assessment includes the identification, analysis, evaluation, handling and documentation of risks with regard to the following aspects: • Protection needs regarding the confidentiality, integrity, availability and authenticity of information processed, stored or transmitted by the third party; • Impact of a protection breach on the provision of the cloud service; • The Cloud Service Provider's dependence on the service provider or supplier for the scope, complexity and uniqueness of the service purchased, including the consideration of possible alternatives.		
The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment periodically to identify and evaluate risks.	No exceptions noted.
	Inspected the risk assessment documentation to determine that the organization's risk assessment considered the operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.

bernardo@hotmaker.ro

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Identity and Access Management Policy and risk assessment documentation to determine that a risk assessment was documented and evaluated the following risk areas: • Administration of rights profiles, approval and assignment of access, and access authorizations • Development, testing, and release of changes • Operation of the system components	No exceptions noted.
	Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas: • Processing, storage, and transmission of data of cloud customers with different protection needs • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources • Attacks via access points, including interfaces accessible from public networks • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons • Dependencies on subservice organizations	No exceptions noted.
Cloud Subprocessor security and privacy risk is assessed via periodic assessment of subprocessor control environment.	Inspected the VSA Guidelines and documentation for a sample of cloud subprocessors to determine that annual assessments of security and privacy risks in subprocessor control environments were performed.	No exceptions noted.

bernard@abtmaker.io

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Subprocessor performance is regularly assessed and monitored via periodic business reviews.	Inspected the Subprocessor Business Reports for a sample of subprocessors to determine that subprocessor performance was regularly assessed and monitored through business reviews.	No exceptions noted.
The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
	Inspected NDA acknowledgements for a sample of external parties to determine that the organization established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.

SSO-03: Directory of Service Providers and Suppliers

The Cloud Service Provider maintains a directory for controlling and monitoring the service providers and suppliers who contribute services to the delivery of the cloud service. The following information is maintained in the directory:

- Company name;
- Address;
- Locations of data processing and storage;
- Responsible contact person at the service provider/supplier;
- Responsible contact person at the cloud service provider;
- Description of the service;
- Classification based on the risk assessment;
- Beginning of service usage; and
- Proof of compliance with contractually agreed requirements.

The information in the list is checked at least annually for completeness, accuracy and validity.

bernard@bonnaker.io

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Where the organization is a data processor, the organization maintains and makes available a list of subprocessors and updates that list, as contractually required.	Inspected the subprocessor list and version history on the external web page to determine that, where the organization was a data processor, the organization maintained and made available a list of subprocessors and updated that list as contractually required.	No exceptions noted.
SSO-04: Monitoring of Compliance with Requirements The Cloud Service Provider monitors compliance with information security requirements and applicable legal and regulatory requirements in accordance with policies and instructions concerning controlling and monitoring of third-parties. Monitoring includes a regular review of the following evidence to the extent that such evidence is to be provided by third parties in accordance with the contractual agreements: • Reports on the quality of the service provided; • Certificates of the management systems' compliance with international standards; • Independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and • Records of the third parties on the handling of vulnerabilities, security incidents and malfunctions. The frequency of the monitoring corresponds to the classification of the third party based on the risk assessment conducted by the Cloud Service Provider (cf. SSO-02). The results of the monitoring are included in the review of the third party's risk assessment. Identified violations and deviations are subjected to analysis, evaluation and treatment in accordance with the risk management procedure (cf. OIS-07).		
Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Inspected documentation of data center security reviews performed for all in-scope data centers to determine that data center security measures were assessed at least annually and the results were reviewed by executive management.	No exceptions noted.
Cloud Subprocessor security and privacy risk is assessed via periodic assessment of subprocessor control environment.	Inspected the VSA Guidelines and documentation for a sample of cloud subprocessors to determine that annual assessments of security and privacy risks in subprocessor control environments were performed.	No exceptions noted.

bernard@boitmaker.nl

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Subprocessor performance is regularly assessed and monitored via periodic business reviews.	Inspected the Subprocessor Business Reports for a sample of subprocessors to determine that subprocessor performance was regularly assessed and monitored through business reviews.	No exceptions noted.
The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
	Inspected NDA acknowledgements for a sample of external parties to determine that the organization established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.
The Privacy, Safety Security Org (PSS) takes a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	Inspected the VSA Guidelines to determine that the PSS had a documented, risk-based approach for reviewing vendor security practices and product security posture, including automated procedures for system configuration, performance, response times, and incident recovery.	No exceptions noted.
	Inspected the VSA review documentation, QBRs, and MBRs for a sample of vendors to determine that both automated and manual assessments were performed based on data sensitivity.	No exceptions noted.

bernard@bonnaker.io

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
SSO-05: Exit Strategy for the Receipt of Benefits The Cloud Service Provider has defined and documented exit strategies for the purchase of services where the risk assessment of the service providers and suppliers regarding the scope, complexity and uniqueness of the purchased service resulted in a very high dependency (cf. Supplementary Information). Exit strategies are aligned with operational continuity plans and include the following aspects: • Analysis of the potential costs, impacts, resources and timing of the transition of a purchased service to an alternative service provider or supplier; • Definition and allocation of roles, responsibilities and sufficient resources to perform the activities for a transition; • Definition of success criteria for the transition; and • Definition of indicators for monitoring the performance of services, which should initiate the withdrawal from the service if the results are unacceptable.		
The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
	Inspected NDA acknowledgements for a sample of external parties to determine that the organization established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.
The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment periodically to identify and evaluate risks.	No exceptions noted.
	Inspected the risk assessment documentation to determine that the organization's risk assessment considered the operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.

bernard@...otmaker.nl

5.12 Control and Monitoring of Service Providers and Suppliers (SSO): Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subservice provider) can access and monitor the agreed services and security requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Identity and Access Management Policy and risk assessment documentation to determine that a risk assessment was documented and evaluated the following risk areas: • Administration of rights profiles, approval and assignment of access, and access authorizations • Development, testing, and release of changes • Operation of the system components	No exceptions noted.
	Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas: • Processing, storage, and transmission of data of cloud customers with different protection needs • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources • Attacks via access points, including interfaces accessible from public networks • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons • Dependencies on subservice organizations	No exceptions noted.
Subprocessor performance is regularly assessed and monitored via periodic business reviews.	Inspected the Subprocessor Business Reports for a sample of subprocessors to determine that subprocessor performance was regularly assessed and monitored through business reviews.	No exceptions noted.

bernard@abtmaker.io

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
SIM-01: Policy for Security Incident Management Policies and instructions with technical and organizational safeguards are documented, communicated and provided in accordance with SP-01 to ensure a fast, effective and proper response to all known security incidents. The Cloud Service Provider defines guidelines for the classification, prioritization and escalation of security incidents and creates interfaces to the incident management and business continuity management. In addition, the Cloud Service Provider has set up a "Computer Emergency Response Team" (CERT), which contributes to the coordinated resolution of occurring security incidents. Customers affected by security incidents are informed in a timely and appropriate manner.		
The organization provides internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	Inspected the Security Incident Response Policy and incident reporting settings on the intranet to determine that the organization provided internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	No exceptions noted.
The organization has implemented a "follow the sun" model for its Security & Privacy Incident Response teams to ensure 24x7 coverage & continuity of operations.	Inspected 24/7 on-call schedules for Security and Privacy Incident Response teams to determine that the organization implemented a "follow the sun" model for its Security and Privacy Incident Response teams that ensured 24/7 coverage and continuity of operations.	No exceptions noted.
The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.

bernard@hotmaker.id

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	No exceptions noted.
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.

bernard@bluemaker.io

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization maintains a framework that defines how to organize a response to security and privacy incidents.	Inspected internal incident response web pages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and privacy incidents.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
The organization has established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.	Inspected the security team intranet web page and schedule to determine that a dedicated security team was established to engage in the security and privacy of customer data and manage security 24/7 worldwide.	No exceptions noted.

bernard@bunker.rip

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has a dedicated team responsible for managing security & privacy incidents.	Inspected the security team's internal web page and schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.	No exceptions noted.
SIM-02: Processing of Security Incidents Subject matter experts of the Cloud Service Provider, together with external security providers where appropriate, classify, prioritize and perform root-cause analyses for events that could constitute a security incident.		
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	No exceptions noted.
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.

bernard@pentmaker.io

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.
The organization maintains a framework that defines how to organize a response to security and privacy incidents.	Inspected internal incident response web pages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and privacy incidents.	No exceptions noted.
The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.
The organization has a dedicated team responsible for managing security & privacy incidents.	Inspected the security team's internal web page and schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.	No exceptions noted.

bernard@bonnaker.ro

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
SIM-03 Documentation and Reporting of Security Incidents After a security incident has been processed, the solution is documented in accordance with the contractual agreements and the report is sent to the affected customers for final acknowledgement or, if applicable, as confirmation.		
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	No exceptions noted.
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.

bernard@automaker.io

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.
The organization has a dedicated team responsible for managing security & privacy incidents.	Inspected the security team's internal web page and schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.	No exceptions noted.
The organization maintains a framework that defines how to organize a response to security and privacy incidents.	Inspected internal incident response web pages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and privacy incidents.	No exceptions noted.
SIM-04: Duty of the Users to Report Security Incidents to a Central Body The Cloud Service Provider informs employees and external business partners of their obligations. If necessary, they agree to or are contractually obliged to report all security events that become known to them and are directly related to the cloud service provided by the Cloud Service Provider to a previously designated central office of the Cloud Service Provider promptly. In addition, the Cloud Service Provider communicates that "false reports" of events that do not subsequently turn out to be incidents do not have any negative consequences.		

bernard@bothmakerin

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization provides external users with mechanisms to report security issues, incidents and concerns.	Inspected Google support documentation and external support resources to determine that the organization provided external users with mechanisms to report security issues, incidents, and concerns.	No exceptions noted.
The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Inspected the Google Cloud Platform (GCP) ToS to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications such as the ToS.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications.	No exceptions noted.
The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
	Inspected NDA acknowledgements for a sample of external parties to determine that the organization established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.

bernard@bonfaker.ro

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has established a code of conduct that is reviewed and updated as needed.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Data Security Policy, and Security and Resilience Policy to determine that the organization had established internal privacy and information security policies, as well as a Code of Conduct, that were reviewed and updated as needed.	No exceptions noted.
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	No exceptions noted.
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.

bernard@bonnaker.fr

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.
SIM-05: Evaluation and Learning Process Mechanisms are in place to measure and monitor the type and scope of security incidents and to report them to support agencies. The information obtained from the evaluation is used to identify recurrent or significant incidents and to identify the need for further protection.		
Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	No exceptions noted.

bernard@bolmaker.ro

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts.	Inspected log monitoring dashboards, audit logging configurations, and an example log to determine that audit logs were retained for events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support log auditability for detecting potentially suspicious or malicious activities.	No exceptions noted.
	Inspected audit logging and monitoring tools at both tenant level and Google internal levels, along with a sample of audit logs, to determine that retained logs covered privileged user access activities, authorized access attempts, and unauthorized access attempts to support security incident investigation.	No exceptions noted.
Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Inspected the Security and Privacy Incident Response Policy, Security Logging Policy, and Device Configuration Guidelines to determine that monitoring tools were documented to send automated alerts to operational personnel based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.
	Inspected alert configurations and an example alert sent from monitoring tools to operational personnel to determine that automated alerts were sent based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.

bernard@bonnaker.ro

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Mechanisms are in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	Inspected firewall and network configurations, and an example alert, to determine that mechanisms detected and prevented unauthorized devices from connecting to the organization's network.	No exceptions noted.
The organization has a dedicated team responsible for managing security & privacy incidents.	Inspected the security team's internal web page and schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.	No exceptions noted.
Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
	Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents was used to strengthen and improve security controls and prevent future incidents and could be used as examples for information security training.	No exceptions noted.
	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.

bernard@bountaker.io

5.13 Security Incident Management (SIM): Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected security event and incident documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the organization had recovered from the incidents.	No exceptions noted.

bernard@botmaker.fr

5.14 Business Continuity Management (BCM): Plan, implement, maintain and test procedures and measures for business continuity and emergency management.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
BCM-01: Top Management Responsibility The top management (or a member of the top management) of the Cloud Service Provider is named as the process owner of business continuity and emergency management and is responsible for establishing the process within the company as well as ensuring compliance with the guidelines. They must ensure that sufficient resources are made available for an effective process. People in management and other relevant leadership positions demonstrate leadership and commitment to this issue by encouraging employees to actively contribute to the effectiveness of continuity and emergency management.		
The organization maintains a framework that defines how to organize a response to security and privacy incidents.	Inspected internal incident response web pages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and privacy incidents.	No exceptions noted.
The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	Inspected the BIA, BC planning documentation, and the organization's ISO 27001 SoA to determine that requirements were established for business continuity measures that maintained the availability of the organization's production infrastructure and services.	No exceptions noted.
	Inspected Disaster Resiliency Testing documentation, including assigned roles, responsibilities, risks, and recovery objectives within the BC Plan, to determine that the organization implemented business continuity measures to maintain the availability of its production infrastructure and services.	No exceptions noted.
	Inspected documented recovery activities in the DR Report to determine that recovery activities were outlined to maintain the availability of the organization's production infrastructure and services.	No exceptions noted.

bernard@bottmaker.io

5.14 Business Continuity Management (BCM): Plan, implement, maintain and test procedures and measures for business continuity and emergency management.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
BCM-02: Business Impact Analysis Policies and Instructions Policies and instructions to determine the impact of any malfunction to the cloud service or enterprise are documented, communicated and made available in accordance with SP-01. The following aspects are considered as minimum: • Possible scenarios based on a risk analysis; • Identification of critical products and services; • Identify dependencies, including processes (including resources required), applications, business partners and third parties; • Capture threats to critical products and services; • Identification of effects resulting from planned and unplanned malfunctions and changes over time; • Determination of the maximum acceptable duration of malfunctions; • Identification of restoration priorities; • Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); • Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and • Estimation of the resources needed for resumption.		
The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected DR and BC planning documentation and testing checklists to determine that DR and BC testing was required to be conducted at least annually and included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
	Inspected DR and BC testing documentation and results for a sample of products to determine that the organization conducted disaster resiliency testing covering reliability, survivability, and recovery at least annually.	Exception noted. For 1 out of 25 Disaster Resiliency Tests sampled, the organization did not provide sufficient documentation confirming that disaster resiliency testing was conducted on an ongoing

bernard@hotmaker.io

5.14 Business Continuity Management (BCM): Plan, implement, maintain and test procedures and measures for business continuity and emergency management.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
		basis (at least annually) to adequately cover reliability, survivability, and recovery. An additional sample of 15 Disaster Resiliency Tests was selected and testing was completed for each of the products in the additional sample.
	Inspected the BIA documentation to determine that potential impacts to business operations were considered.	No exceptions noted.
The organization develops and maintains a risk management framework to manage risk to an acceptable level.	Inspected the risk management guidelines to determine that the organization developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
	Inspected risk management guidelines and the risk assessment documentation to determine that management of the organization evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment periodically to identify and evaluate risks.	No exceptions noted.

bernard@hotmaker.io

5.14 Business Continuity Management (BCM): Plan, implement, maintain and test procedures and measures for business continuity and emergency management.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the risk assessment documentation to determine that the organization's risk assessment considered the operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
	Inspected the Identity and Access Management Policy and risk assessment documentation to determine that a risk assessment was documented and evaluated the following risk areas: • Administration of rights profiles, approval and assignment of access, and access authorizations • Development, testing, and release of changes • Operation of the system components	No exceptions noted.
	Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas: • Processing, storage, and transmission of data of cloud customers with different protection needs • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources • Attacks via access points, including interfaces accessible from public networks • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons • Dependencies on subservice organizations	No exceptions noted.

bernard@bumaker.fr

5.14 Business Continuity Management (BCM): Plan, implement, maintain and test procedures and measures for business continuity and emergency management.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.

bernard@bumaker.fr

BCM-03: Planning Business Continuity

Based on the business impact analysis, a single framework for operational continuity and business plan planning will be implemented, documented and enforced to ensure that all plans are consistent. Planning is based on established standards, which are documented in a "Statement of Applicability".

Business continuity plans and contingency plans take the following aspects into account:
• Defined purpose and scope with consideration of the relevant dependencies;
• Accessibility and comprehensibility of the plans for persons who are to act accordingly;
• Ownership by at least one designated person responsible for review, updating and approval;
• Defined communication channels, roles and responsibilities including notification of the customer;
• Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud infrastructure components and services and alignment with customers);

5.14 Business Continuity Management (BCM): Plan, implement, maintain and test procedures and measures for business continuity and emergency management.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
• Methods for putting the plans into effect; • Continuous process improvement; and • Interfaces to Security Incident Management.		
BigQuery Omni is hosted on third-party infrastructure, and business continuity planning is the responsibility of the subservice organizations.	Not applicable.	Not applicable.
The organization has geographically dispersed personnel responsible for managing security incidents.	Inspected the security team intranet web page and schedule to determine that personnel were geographically dispersed to manage security incidents.	No exceptions noted.
The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	Inspected the BIA, BC planning documentation, and the organization's ISO 27001 SoA to determine that requirements were established for business continuity measures that maintained the availability of the organization's production infrastructure and services.	No exceptions noted.
	Inspected Disaster Resiliency Testing documentation, including assigned roles, responsibilities, risks, and recovery objectives within the BC Plan, to determine that the organization implemented business continuity measures to maintain the availability of its production infrastructure and services.	No exceptions noted.
	Inspected documented recovery activities in the DR Report to determine that recovery activities were outlined to maintain the availability of the organization's production infrastructure and services.	No exceptions noted.

bernard@bdtmaker.io

5.14 Business Continuity Management (BCM): Plan, implement, maintain and test procedures and measures for business continuity and emergency management.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the replication tool dashboard; monitoring tool dashboard; and filesystem, datastore, and network configurations for products and networks to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities.	No exceptions noted.
	Inspected the CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of customer data through the implementation of backups within the organization's information processing resources.	No exceptions noted.
The organization maintains a framework that defines how to organize a response to security and privacy incidents.	Inspected internal incident response web pages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and privacy incidents.	No exceptions noted.
BCM-04: Verification, Updating and Testing of the Business Continuity Plan The business impact analysis, business continuity plans and contingency plans are reviewed, updated and tested on a regular basis (at least annually) or after significant organizational or environmental changes. Tests involve affected customers (tenants) and relevant third parties. The tests are documented and results are taken into account for future operational continuity measures.		
BigQuery Omni is hosted on third-party infrastructure, and verification, updating, and testing of the business continuity plan are the responsibility of the subservice organizations.	Not applicable.	Not applicable.

bernard@bumaker.ru

5.14 Business Continuity Management (BCM): Plan, implement, maintain and test procedures and measures for business continuity and emergency management.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected DR and BC planning documentation and testing checklists to determine that DR and BC testing was required to be conducted at least annually and included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
	Inspected DR and BC testing documentation and results for a sample of products to determine that the organization conducted disaster resiliency testing covering reliability, survivability, and recovery at least annually.	Exception noted. For 1 out of 25 Disaster Resiliency Tests sampled, the organization did not provide sufficient documentation confirming that disaster resiliency testing was conducted on an ongoing basis (at least annually) to adequately cover reliability, survivability, and recovery. An additional sample of 15 Disaster Resiliency Tests was selected and testing was completed for each of the products in the additional sample.
	Inspected the BIA documentation to determine that potential impacts to business operations were considered.	No exceptions noted.

bernard@bornaker.ro

5.15 Compliance (COM): Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
COM-01: Identification of Applicable Legal, Regulatory, Self-Imposed or Contractual Requirements The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service as well as the Cloud Service Provider's procedures for complying with these requirements are explicitly defined and documented.		
The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Inspected the Google Cloud Platform (GCP) ToS to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications such as the ToS.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications.	No exceptions noted.
The approach to meeting relevant statutory, regulatory, and contractual requirements is defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	Inspected the product launch process, the relevant Google Cloud ToS, and the internal cloud compliance website to determine that the organization's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	No exceptions noted.

bernard@bothmarr.io

5.15 Compliance (COM): Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
COM-02: Policy for Planning and Conducting Audits Policies and instructions for planning and conducting audits are documented, communicated and made available in accordance with SP-01 and address the following aspects: • Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; • Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and • Logging and monitoring of activities.		
The organization plans and coordinates system security-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users.	Inspected planning documentation and stakeholder coordination documentation to determine that the organization planned and coordinated system security-related audits with the relevant stakeholders before conducting such activities, in order to reduce the impact on internal and consumer users.	No exceptions noted.
The organization has an internal audit function and regularly engages independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	Inspected internal audit program manuals and compliance guidelines to determine that an internal audit function was in place, regularly engaging independent third parties to review the effectiveness of the organization's information security and privacy practices, with findings and corrective actions tracked and communicated to stakeholders.	No exceptions noted.
	Inspected security compliance certifications from independent audits to determine that the organization regularly engaged third parties for independent reviews of its information security practices.	No exceptions noted.

bernard@mailmaker.io

5.15 Compliance (COM): Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
COM-03: Internal Audits of the Information Security Management System Subject matter experts check the compliance of the information security management system at regular intervals, at least annually, with the relevant and applicable legal, regulatory, self-imposed or contractual requirements (cf. COM-01) as well as compliance with the policies and instructions (cf. SP-01) within their scope of responsibility (cf. OIS-01) through internal audits. Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18).		
The organization has an established Internal Audit function which evaluates management's compliance with security controls.	Inspected the Internal Audit report to determine that the organization established an Internal Audit function that evaluated management's compliance with security controls at least annually.	No exceptions noted.

bernard@bumaker.io

5.15 Compliance (COM): Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization periodically reviews and validates the design, operation and control record of in-scope compliance controls.	Inspected the ISMS and risk assessment documentation to determine that the design, operation, and control record of in-scope compliance controls were reviewed and validated at least annually, with corrective actions taken based on relevant findings.	No exceptions noted.
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, Priority Guidelines, and the online register of known vulnerabilities to determine that the organization implemented a vulnerability management program, including third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring that remediation plans were developed and implemented for all critical and high-security deficiencies and tracked within internal tools, and that security patches were applied based on vulnerability severity and assigned CVSS scores.	No exceptions noted.
	Inspected vulnerability scanning frequency configurations, example monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
	Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.

bernard@boomtaker.io

5.15 Compliance (COM): Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability planning meetings to determine that security teams met regularly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
The organization has an internal audit function and regularly engages independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	Inspected internal audit program manuals and compliance guidelines to determine that an internal audit function was in place, regularly engaging independent third parties to review the effectiveness of the organization's information security and privacy practices, with findings and corrective actions tracked and communicated to stakeholders.	No exceptions noted.
	Inspected security compliance certifications from independent audits to determine that the organization regularly engaged third parties for independent reviews of its information security practices.	No exceptions noted.
Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies on the intranet to determine that policies were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
	Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.

bernard@bbrtaker.ru

5.15 Compliance (COM): Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
COM-04: Information on Information Security Performance and Management Assessment of the ISMS The top management of the Cloud Service Provider is regularly informed about the information security performance within the scope of the ISMS in order to ensure its continued suitability, adequacy and effectiveness. The information is included in the management review of the ISMS and is performed at least once a year.		
Information security is managed by an executive who is dedicated to Security, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.	Inspected Security organizational charts to determine that information security was managed by a dedicated executive, independent of Information Technology (IT) responsibility, with authority to escalate security issues to the board level as needed.	No exceptions noted.
	Inspected an example meeting calendar invite and agenda for a recent Security and Privacy team meeting to determine that a Security executive met with relevant personnel to discuss security issues and had the option to escalate concerns to the board level as needed.	No exceptions noted.
All board of directors' exercise independent judgment. The independent/non-employee board of directors also demonstrate independence from management in exercising oversight of the development and performance of internal control.	Inspected the Corporate Governance Guidelines and an example board meeting calendar invite and agenda to determine that all board members exercised independent judgment, with independent/non-employee directors demonstrating independence from management in oversight of internal control.	No exceptions noted.

bernard@bormaker.fr

5.15 Compliance (COM): Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the Corporate Governance Guidelines and the board listing on the Investor Relations web page to determine that the board demonstrated independence from management.	No exceptions noted.
The organization has an established Internal Audit function which evaluates management's compliance with security controls.	Inspected the Internal Audit report to determine that the organization established an Internal Audit function that evaluated management's compliance with security controls at least annually.	No exceptions noted.

bernard@bothAker.io

5.16 Dealing with Investigation Requests from Government Agencies (INQ): Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
INQ-01: Legal Assessment of Investigative Inquiries Investigation requests from government agencies are subjected to a legal assessment by subject matter experts of the Cloud Service Provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken.		
The organization establishes designated legal counsel and Government Affairs officials in order to maintain appropriate contacts with law enforcement authorities.	Inspected internal guidance and web pages to determine that the organization designated legal counsel and Government Affairs officials in order to maintain appropriate contacts with law enforcement authorities.	No exceptions noted.
Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon in the contract, unless such notification is otherwise prohibited.	Inspected Government Requests for Cloud Customer Data, the Google Cloud ToS, and internal documentation to determine that mechanisms were in place to notify customers of data requests in accordance with contractually agreed procedures and time frames, when legally required to disclose PII, unless notification was otherwise prohibited, and to produce data as required by applicable law, regulation, legal process, or enforceable government request.	No exceptions noted.
	Inspected the case management system, customer disclosure notes, and an example investigative request case to determine that mechanisms were in place to notify customers of data requests in accordance with contractually agreed procedures and time frames when legally required to disclose PII, unless such notification was otherwise prohibited, and that procedures were established to produce data as required by applicable law, regulation, legal process, or enforceable government requests.	No exceptions noted.

bernard@mothaser.no

5.16 Dealing with Investigation Requests from Government Agencies (INQ): Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	Inspected the Information Security and Privacy Incident Response Policy and the procedures for reporting an incident on the Company intranet to determine that the organization maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
	Inspected the requirement for timely notifications of data breaches to affected customers, in accordance with disclosure laws or contractual agreements, within the CDPA shared with customers to determine that the organization communicated policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
INQ-02: Informing Cloud Customers about Investigation Requests The Cloud Service Provider informs the affected Cloud Customer(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the Cloud Service.		
Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon in the contract, unless such notification is otherwise prohibited.	Inspected Government Requests for Cloud Customer Data, the Google Cloud ToS, and internal documentation to determine that mechanisms were in place to notify customers of data requests in accordance with contractually agreed procedures and time frames, when legally required to disclose PII, unless notification was otherwise prohibited, and to produce data as required by applicable law, regulation, legal process, or enforceable government request.	No exceptions noted.

bernard@bunnaker.io

5.16 Dealing with Investigation Requests from Government Agencies (INQ): Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected the case management system, customer disclosure notes, and an example investigative request case to determine that mechanisms were in place to notify customers of data requests in accordance with contractually agreed procedures and time frames when legally required to disclose PII, unless such notification was otherwise prohibited, and that procedures were established to produce data as required by applicable law, regulation, legal process, or enforceable government requests.	No exceptions noted.
INQ-03: Conditions for Access to or Disclosure of Data in Investigation Requests Access to or disclosure of cloud customer data in connection with government investigation requests is subject to the proviso that the Cloud Service Provider's legal assessment has shown that an applicable and valid legal basis exists and that the investigation request must be granted on that basis.		
The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	Inspected the Information Security and Privacy Incident Response Policy and the procedures for reporting an incident on the Company intranet to determine that the organization maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
	Inspected the requirement for timely notifications of data breaches to affected customers, in accordance with disclosure laws or contractual agreements, within the CDPA shared with customers to determine that the organization communicated policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.

bernard@botmaker.ro

5.16 Dealing with Investigation Requests from Government Agencies (INQ): Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon in the contract, unless such notification is otherwise prohibited.	Inspected Government Requests for Cloud Customer Data, the Google Cloud ToS, and internal documentation to determine that mechanisms were in place to notify customers of data requests in accordance with contractually agreed procedures and time frames, when legally required to disclose PII, unless notification was otherwise prohibited, and to produce data as required by applicable law, regulation, legal process, or enforceable government request.	No exceptions noted.
	Inspected the case management system, customer disclosure notes, and an example investigative request case to determine that mechanisms were in place to notify customers of data requests in accordance with contractually agreed procedures and time frames when legally required to disclose PII, unless such notification was otherwise prohibited, and that procedures were established to produce data as required by applicable law, regulation, legal process, or enforceable government requests.	No exceptions noted.

INQ-04: Limiting Access to or Disclosure of Data in Investigation Requests

The Cloud Service Provider's procedures for setting up access to or disclosure of cloud customer data as part of an investigation request, ensure that government agencies only have access to the data they need to investigate.

If no clear limitation of the data is possible, the Cloud Service Provider anonymizes or pseudonymizes the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request.

bernard@bootmaker.ro

5.16 Dealing with Investigation Requests from Government Agencies (INQ): Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	Inspected the Information Security and Privacy Incident Response Policy and the procedures for reporting an incident on the Company intranet to determine that the organization maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
	Inspected the requirement for timely notifications of data breaches to affected customers, in accordance with disclosure laws or contractual agreements, within the CDPA shared with customers to determine that the organization communicated policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon in the contract, unless such notification is otherwise prohibited.	Inspected Government Requests for Cloud Customer Data, the Google Cloud ToS, and internal documentation to determine that mechanisms were in place to notify customers of data requests in accordance with contractually agreed procedures and time frames, when legally required to disclose PII, unless notification was otherwise prohibited, and to produce data as required by applicable law, regulation, legal process, or enforceable government request.	No exceptions noted.
	Inspected the case management system, customer disclosure notes, and an example investigative request case to determine that mechanisms were in place to notify customers of data requests in accordance with contractually agreed procedures and time frames when	No exceptions noted.

bernard@bunmaker.io

5.16 Dealing with Investigation Requests from Government Agencies (INQ): Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	legally required to disclose PII, unless such notification was otherwise prohibited, and that procedures were established to produce data as required by applicable law, regulation, legal process, or enforceable government requests.	

bernard@botmaker.io

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
PSS-01: Guidelines and Recommendations for Cloud Customers The Cloud Service Provider provides cloud customers with guidelines and recommendations for the secure use of the cloud service provided. The information contained therein is intended to assist the cloud customer in the secure configuration, installation and use of the cloud service, to the extent applicable to the cloud service and the responsibility of the cloud user. The type and scope of the information provided will be based on the needs of subject matter experts of the cloud customers who set information security requirements, implement them or verify the implementation (e.g., IT, Compliance, Internal Audit). The information in the guidelines and recommendations for the secure use of the cloud service address the following aspects, where applicable to the cloud service: • Instructions for secure configuration; • Information sources on known vulnerabilities and update mechanisms; • Error handling and logging mechanisms; • Authentication mechanisms; • Roles and rights concept including combinations that result in an elevated risk; and • Services and functions for administration of the cloud service by privileged users. The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.		
The organization provides information pertaining to the shared responsibilities of both itself and the cloud service customer.	Inspected the CDPA on the organization's web page to determine that the organization provided information pertaining to the shared responsibilities of both itself and the cloud service customer.	No exceptions noted.
Customer responsibilities are described on the organization's product websites or in system documentation.	Inspected customer responsibilities on the organization's websites and in system documentation, as well as the GCP ToS, that was accessible by internal and external customers to determine that customer responsibilities were described on the organization's product websites or in system documentation.	No exceptions noted.

bernard@bothriker.ro

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization provides customers with information regarding default encryption methods used to protect user data. Additional applications of cryptographic protections are documented and shared through public sites.	Inspected the CDPA and the organization's Default Encryption at Rest web page to determine that information regarding default encryption methods used to protect customer data was provided to customers and additional applications of cryptographic protections were documented and shared through public sites.	No exceptions noted.
The organization provides external users with mechanisms to report security issues, incidents and concerns.	Inspected Google support documentation and external support resources to determine that the organization provided external users with mechanisms to report security issues, incidents, and concerns.	No exceptions noted.
Changes to customer facing services that may affect confidentiality, processing integrity and/or availability are communicated to relevant personnel and impacted customers.	Inspected alert notifications and change ticket communication history for a sample of changes to customer-facing services to determine that relevant personnel were notified of changes that could have affected security, confidentiality, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker web page, and the customer-facing log of vulnerabilities to determine that impacted customers were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.
PSS-02: Identification of Vulnerabilities of the Cloud Service The Cloud Service Provider applies appropriate measures to check the cloud service for vulnerabilities which might have been integrated into the cloud service during the software development process. The procedures for identifying such vulnerabilities are part of the software development process and, depending on a risk assessment, include the following activities:		

bernard@dormakaba.ch

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
• Static Application Security Testing; • Dynamic Application Security Testing; • Code reviews by the Cloud Service Provider's subject matter experts; and • Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service. The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.		
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, Priority Guidelines, and the online register of known vulnerabilities to determine that the organization implemented a vulnerability management program, including third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring that remediation plans were developed and implemented for all critical and high-security deficiencies and tracked within internal tools, and that security patches were applied based on vulnerability severity and assigned CVSS scores.	No exceptions noted.
	Inspected vulnerability scanning frequency configurations, example monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
	Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.

bernard@bolmaker.io

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability planning meetings to determine that security teams met regularly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
Penetration tests are performed using a defined methodology and frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes.	Inspected the semi-annual and continuous penetration test results to determine that tests were performed at least every six months by independent external auditors, using a methodology and frequency aligned with compliance requirements and customer commitments.	No exceptions noted.
	Inspected remediation plans for vulnerabilities identified during the semi-annual and continuous penetration test to determine that corrective actions were taken in accordance with vulnerability management processes and that plans were developed and changes were implemented to address, at a minimum, all high and medium vulnerabilities.	No exceptions noted.
The organization has policies and guidelines governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy, the Security Requirements for Outsourced Software Development Policy, and the Source Code Guidelines, to determine that the organization had established policies and guidelines governing the secure development lifecycle, including requirements for outsourced development.	No exceptions noted.

bernard@bornaker.ro

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Changes to the organization's systems are tested before being deployed.	Inspected testing notes within change request tickets for a sample of system changes to determine that changes to the organization's systems were tested prior to deployment.	No exceptions noted.
PSS-03: Online Register of Known Vulnerabilities The Cloud Service Provider operates or refers to a daily updated online register of known vulnerabilities that affect the Cloud Service Provider and assets provided by the Cloud Service Provider that the cloud customers have to install, provide or operate themselves under the customers responsibility. The presentation of the vulnerabilities follows the Common Vulnerability Scoring System (CVSS). The online register is easily accessible to any cloud customer. The information contained therein forms a suitable basis for risk assessment and possible follow-up measures on the part of cloud users for each vulnerability, it is indicated whether software updates (e.g., patch, update) are available, when they will be rolled out and whether they will be deployed by the Cloud Service Provider, the cloud customer or both of them together.		
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, Priority Guidelines, and the online register of known vulnerabilities to determine that the organization implemented a vulnerability management program, including third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring that remediation plans were developed and implemented for all critical and high-security deficiencies and tracked within internal tools, and that security patches were applied based on vulnerability severity and assigned CVSS scores.	No exceptions noted.

bernardobotmaker.in

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected vulnerability scanning frequency configurations, example monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
	Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability planning meetings to determine that security teams met regularly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
Changes to customer facing services that may affect confidentiality, processing integrity and/or availability are communicated to relevant personnel and impacted customers.	Inspected alert notifications and change ticket communication history for a sample of changes to customer-facing services to determine that relevant personnel were notified of changes that could have affected security, confidentiality, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker web page, and the customer-facing log of vulnerabilities to determine that impacted customers were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.

bernard@bgrnaker.ru

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.
	Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.

bernard@bottmaker.ru

PSS-04: Error Handling and Logging Mechanisms

The cloud service provider is equipped with error handling and logging mechanisms. These enable cloud users to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides. The information is detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service:

• Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs);

• Malfunctions during processing of automatic or manual actions; and

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
• Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorization, cryptography, and communication security. The logged information is protected from unauthorized access and modification and can be deleted by the Cloud Customer. If the cloud customer is responsible for the activation or type and scope of logging, the Cloud Service Provider must provide appropriate logging capabilities.		
Security event logs are protected, and access is restricted to authorized personnel.	Inspected the Security Logging Policy, security event log protection configuration, and the list of users with access to security event logs and their job titles to determine that security event logs were protected and access was restricted to authorized personnel.	No exceptions noted.
Audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts.	Inspected log monitoring dashboards, audit logging configurations, and an example log to determine that audit logs were retained for events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support log auditability for detecting potentially suspicious or malicious activities.	No exceptions noted.
	Inspected audit logging and monitoring tools at both tenant level and Google internal levels, along with a sample of audit logs, to determine that retained logs covered privileged user access activities, authorized access attempts, and unauthorized access attempts to support security incident investigation.	No exceptions noted.

bernard@bountaker.io

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	Inspected the Information Security and Privacy Incident Response Policy and the procedures for reporting an incident on the Company intranet to determine that the organization maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
	Inspected the requirement for timely notifications of data breaches to affected customers, in accordance with disclosure laws or contractual agreements, within the CDPA shared with customers to determine that the organization communicated policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
At a minimum, security event logs must include the following: user ID, event type, timestamp, success/failure indication, event origination, and affected data/resource identifier. Security event logs are retained for a minimum of one (1) year.	Inspected log management tool configurations and example logs to determine that audit logs included, at a minimum, user ID, event type, timestamp, success or failure indication, event origination, and affected data or resource identifier and that logs were retained for at least one year.	No exceptions noted.
	Inspected the Corporate Activity Retention Guidelines, log retention configurations, and example audit logs to determine that audit logs were retained for at least one year and that log data was deleted once it was no longer needed for its original purpose.	No exceptions noted.

bernard@bookmaker.fm

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization monitors its networks and systems for threats to information security.	Inspected the Security Logging Policy, log monitoring configurations, and incident response on-call schedule to determine that the organization monitored its networks and systems for information security threats.	No exceptions noted.
	Inspected job titles and organizational structures for a sample of personnel with logical access to audit logs to determine that access was restricted to authorized personnel.	No exceptions noted.
Network traffic is monitored through a combination of automated and manual controls and processes to detect anomalous network events which could indicate potential malicious activity.	Inspected diagrams, dashboards, and an example alert to determine that network traffic was monitored through automated and manual controls to detect anomalous events that could indicate malicious activity.	No exceptions noted.
PSS-05: Authentication Mechanisms The Cloud Service Provider provides authentication mechanisms that can force strong authentication (e.g., two or more factors) for users, IT components or applications within the cloud users' area of responsibility. These authentication mechanisms are set up at all access points that allow users, IT components or applications to interact with the cloud service. For privileged users, IT components or applications, these authentication mechanisms are enforced.		
Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.	Inspected the authentication configuration enforcing user IDs, passwords, security keys, and/or valid certificates to determine that logical access to organization-owned network devices was authenticated through enforced methods.	No exceptions noted.

bernard@bothAker.fr

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
External system users are identified and authenticated via the Google Accounts or the BYOID authentication system before access is granted.	Inspected the configuration used to identify and authenticate external system users via Google Accounts or the BYOID authentication system to determine that users were identified and authenticated before being granted access to cloud services.	No exceptions noted.
	Inspected the customer account creation process to determine that external system users created their own passwords and were identified and authenticated via Google Accounts or the BYOID authentication system before accessing cloud services.	No exceptions noted.
Personnel access to sensitive internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	Inspected the Account Authentication Guidelines to determine that personnel access to sensitive internal systems and applications required two-factor authentication using a distinct user ID, password, and a security key or certificate.	No exceptions noted.
	Inspected the code enforcing user authentication prior to certificate issuance to determine that personnel access to sensitive internal systems and applications required two-factor authentication with a distinct user ID, password, and security key or certificate and that certificates were generated only after successful two-factor authentication for single sign-on.	No exceptions noted.

bernard@bunnaker.fr

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
PSS-06: Session Management To protect confidentiality, availability, integrity and authenticity during interactions with the cloud service, a suitable session management system is used that at least corresponds to the state-of-the-art and is protected against known attacks. Mechanisms are implemented that invalidate a session after it has been detected as inactive. The inactivity can be detected by time measurement. In this case, the time interval can be configured by the Cloud Service Provider or – if technically possible – by the cloud customer.		
The organization has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	Inspected documented logical and physical network diagrams to determine that the organization required mechanisms by default to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.
	Inspected web browser encryption settings for cloud services and the default system configuration settings within the cloud customer interface that enforced session timeouts to determine that the organization had implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.
PSS-07: Confidentiality of Authentication Information If passwords are used as authentication information for the cloud service, their confidentiality is ensured by the following procedures: • Users can initially create the password themselves or must change an initial password when logging in to the cloud service for the first time. An initial password loses its validity after a maximum of 14 days. • When creating passwords, compliance with the length and complexity requirements of the Cloud Service Provider (cf. IDM-09) or the cloud customer is technically enforced. • The user is informed about changing or resetting the password. • The server-side storage takes place using state-of-the-art cryptographically strong hash functions in combination with at least 32-bit long salt values.		

bernard@hotmaker.ro

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has a password change system that enforces its password guidelines.	Inspected the Guidelines for Google Passwords document and performed a password change to determine that the password change system enforced guidelines as defined in relevant security policies.	No exceptions noted.
	Observed a user attempt to change their password without meeting requirements to determine that an error message was displayed and the password change was unsuccessful.	No exceptions noted.
The organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Guidelines for Google Passwords document to determine that formal guidelines for passwords were established to govern the management and use of authentication mechanisms.	No exceptions noted.
	Inspected SSH idle time configurations on servers to determine that they were configured to enforce password requirements according to formal authentication guidelines.	No exceptions noted.
	Inspected corporate endpoint configurations to determine that users were locked out after a maximum of 15 minutes of inactivity in accordance with formal guidelines for managing authentication mechanisms.	No exceptions noted.
	Inspected the authentication configurations to determine that passwords were transmitted and stored using encrypted procedures according to formal password management guidelines.	No exceptions noted.

bernard@bumaker.fr

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Customer data that is uploaded or created is encrypted at rest.	Inspected the organization's Cryptographic Policy and default encryption-at-rest web page to determine that customer data uploaded or created was required to be encrypted at rest according to storage-level encryption requirements.	No exceptions noted.
	Inspected data backup encryption configurations and encryption settings for storage devices containing customer data to determine that uploaded and created customer data was encrypted at rest.	No exceptions noted.
	Inspected the Customer-Managed Encryption Keys guidance web page to determine that encryption keys could be controlled by the end user.	No exceptions noted.
PSS-08: Roles and Rights Concept The Cloud Service Provider provides cloud users with a roles and rights concept for managing access rights. It describes rights profiles for the functions provided by the cloud service. The rights profiles are suitable for enabling cloud users to manage access authorizations and permissions in accordance with the principle of least-privilege and how it is necessary for the performance of tasks ("need-to-know principle") and to implement the principle of functional separation between operational and controlling functions ("separation of duties").		
Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Inspected administrative operations procedures for the organization's cloud computing environment on the external Quickstarts web page to determine that procedures were documented and made available to customers.	No exceptions noted.

bernard@bornaker.ro

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
PSS-09: Authorization Mechanisms Access to the functions provided by the cloud service is restricted by access controls (authorization mechanisms) that verify whether users, IT components, or applications are authorized to perform certain actions. The Cloud Service Provider validates the functionality of the authorization mechanisms before new functions are made available to cloud users and in the event of changes to the authorization mechanisms of existing functions (cf. DEV-06). The severity of identified vulnerabilities is assessed according to defined criteria based on industry standard metrics (e.g., Common Vulnerability Scoring System) and measures for timely resolution or mitigation are initiated. Vulnerabilities that have not been fixed are listed in the online register of known vulnerabilities (cf. PSS-02).		
The organization has an established policy specifying the use of emergency credentials.	Inspected the Emergency Access Credential Policy to determine that the organization established a policy specifying requirements for the use of emergency credentials.	No exceptions noted.
	Inspected emergency credential expiration configurations and a sample of checkout tickets to determine that credentials required approval from authorized personnel prior to checkout and expired 90 days after issuance.	No exceptions noted.
The organization separates duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	Inspected the Identity and Access Management Policy to determine that the organization separated duties by granting users access based on job responsibilities and least privilege by limiting access to only authorized users.	No exceptions noted.
	Observed an attempt to access a privileged system outside the user's job responsibilities to determine that the organization's separation of duties and principle of least privilege successfully limited access to authorized users only.	No exceptions noted.

bernard@hotmaker.io

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
Personnel access to sensitive internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	Inspected the Account Authentication Guidelines to determine that personnel access to sensitive internal systems and applications required two-factor authentication using a distinct user ID, password, and a security key or certificate.	No exceptions noted.
	Inspected the code enforcing user authentication prior to certificate issuance to determine that personnel access to sensitive internal systems and applications required two-factor authentication with a distinct user ID, password, and security key or certificate and that certificates were generated only after successful two-factor authentication for single sign-on.	No exceptions noted.
PSS-10: Software Defined Networking If the Cloud Service offers functions for software-defined networking (SDN), the confidentiality of the data of the cloud user is ensured by suitable SDN procedures. The Cloud Service Provider validates the functionality of the SDN functions before providing new SDN features to cloud users or modifying existing SDN features. Identified defects are assessed and corrected in a risk-oriented manner.		
The organization has guidelines specifying the security requirements for new and existing information systems.	Inspected the organization's security policies and product documentation to determine that the organization had guidelines specifying the security requirements for new and existing information systems and that the confidentiality of the data of the cloud user was ensured by suitable SDN procedures.	No exceptions noted.

bernard@bcmaker.nl

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization tests, validates, and documents changes to its services prior to deployment to production.	Inspected change tickets for a sample of changes to determine that changes to services were tested, validated, and documented prior to deployment to production.	No exceptions noted.
Penetration tests are performed using a defined methodology and frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes.	Inspected the semi-annual and continuous penetration test results to determine that tests were performed at least every six months by independent external auditors, using a methodology and frequency aligned with compliance requirements and customer commitments.	No exceptions noted.
	Inspected remediation plans for vulnerabilities identified during the semi-annual and continuous penetration test to determine that corrective actions were taken in accordance with vulnerability management processes and that plans were developed and changes were implemented to address, at a minimum, all high and medium vulnerabilities.	No exceptions noted.
The organization provides customers with information regarding default encryption methods used to protect user data. Additional applications of cryptographic protections are documented and shared through public sites.	Inspected the CDPA and the organization's Default Encryption at Rest web page to determine that information regarding default encryption methods used to protect customer data was provided to customers and additional applications of cryptographic protections were documented and shared through public sites.	No exceptions noted.

bernard@bonnaker.ro

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	Inspected documented logical and physical network diagrams to determine that the organization required mechanisms by default to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.
	Inspected web browser encryption settings for cloud services and the default system configuration settings within the cloud customer interface that enforced session timeouts to determine that the organization had implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.
Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Inspected administrative operations procedures for the organization's cloud computing environment on the external Quickstarts web page to determine that procedures were documented and made available to customers.	No exceptions noted.
The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	Inspected the security team intranet web page and schedule to determine that dedicated teams were established to monitor, maintain, manage, and secure the network.	No exceptions noted.
The organization's network security policies and guidelines apply to both physical and virtual networks.	Inspected the Network and Computer Security Policy and Network Device Guidelines to determine that network security policies and guidelines applied to both physical and virtual networks.	No exceptions noted.

bernard@bonnaker.fr

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
PSS-11: Images for Virtual Machines and Containers If cloud customers operate virtual machines or containers with the cloud service, the Cloud Service Provider must ensure the following aspects: • The cloud customer can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this cloud customer can only launch the images or containers released according to these restrictions. • If the Cloud Service Provider provides images of virtual machines or containers to the Cloud Customer, the Cloud Service Provider appropriately informs the Cloud Customer of the changes made to the previous version. • In addition, these images provided by the Cloud Service Provider are hardened according to generally accepted industry standards.		
The organization allows cloud customers to determine data processing and storage location in accordance with contractually defined options.	Inspected the CDPA to determine that cloud customers could select data processing and storage locations based on contractually defined options.	No exceptions noted.
	Inspected the cloud customer portal to determine that cloud customers were allowed to select data processing and storage locations based on contractual availability.	No exceptions noted.
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the network guidelines, production image enforcement tool configurations, customer image restriction cloud portal functionality, and default hardening standards for machines and containers to determine that virtual environments were hardened where the organization held a responsibility as outlined in the shared responsibilities and mechanisms were provided for restricting the selection of default hardened images for virtual machines and containers in the cloud environment.	No exceptions noted.

bernard@otmaker.ro

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.
	Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.
Changes to customer facing services that may affect confidentiality, processing integrity and/or availability are communicated to relevant personnel and impacted customers.	Inspected alert notifications and change ticket communication history for a sample of changes to customer-facing services to determine that relevant personnel were notified of changes that could have affected security, confidentiality, and availability.	No exceptions noted.

bernard@bottmaker.ru

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
	Inspected official product blogs, public community support pages, the issue tracker web page, and the customer-facing log of vulnerabilities to determine that impacted customers were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.
A standard image is utilized for the installation and maintenance of each production server.	Inspected the Change Management Policy, Source Code Guidelines, replication tool configurations, and automated compliance jobs to determine that a standard image was required, maintained, and periodically verified for production servers.	No exceptions noted.
	Inspected monitoring tool configurations to determine that tools monitored production machines, detected deviations from predefined OS configurations, and applied corrections.	No exceptions noted.
PSS-12: Locations of Data Processing and Storage The cloud customer is able to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options. This must be ensured by the cloud architecture.		
The organization specifies and documents the countries and/or data center locations in which customer data might possibly be stored and transferred.	Inspected the available regions on the Google Data Center Locations web page and Google Cloud console to determine that the organization specified and documented potential countries and data center locations for storing and transferring customer data.	No exceptions noted.

bernard@bormaker.ro

5.17 Product Safety and Security (PSS): Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.		
Assigned Controls	**Service Auditor's Tests**	**Results of Tests**
The organization allows cloud customers to determine data processing and storage location in accordance with contractually defined options.	Inspected the CDPA to determine that cloud customers could select data processing and storage locations based on contractually defined options.	No exceptions noted.
	Inspected the cloud customer portal to determine that cloud customers were allowed to select data processing and storage locations based on contractual availability.	No exceptions noted.

bernard@botmaker.io

Section 5

Other Information Provided by Google LLC

bernard@botmaker.io

Management's Response to Testing Exceptions

Assigned Controls	Results of Tests	Management's Response
The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Exception noted. For 1 out of 25 Disaster Resiliency Tests sampled, the organization did not provide sufficient documentation confirming that disaster resiliency testing was conducted on an ongoing basis (at least annually) to adequately cover reliability, survivability, and recovery. An additional sample of 15 Disaster Resiliency Tests was selected and testing was completed for each of the products in the additional sample.	One sampled GCP product did not perform disaster resiliency testing within the reporting period. Management took corrective action and testing will be completed in Q2 2025. Google compliance teams also reviewed DR and BC testing documentation for all other in-scope GCP products to confirm annual testing was performed within the testing period.
Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.	Exceptions noted. The organization did not enforce the automatic revocation of data center access after 2 months of inactivity or the automatic removal after 6 months of inactivity.	Management is cognizant of the system limitations that prevent automatic revocation and removal of data center access rights. Management agrees with the auditor's finding that an automatic revocation and automatic removal of access does not occur after 2 and 6 months of inactivity, respectively. Management believes that the effectiveness of compensating controls are more than sufficient to address the associated control objective. Compensating controls include strict physical access procedures, quarterly physical access reviews, tailgating policies, monitoring of secure areas and automatic revocation of access on termination of employment.

bernardo@hotmaker.io

Assigned Controls	Results of Tests	Management's Response
Data centers are equipped with fire detection alarms and protection equipment.	Exceptions noted. For 3 out of the 8 facilities sampled, the structural components were not constructed with a fire resistance rating of at least 90 minutes.	Management is aware of the limitations of certain data center facilities to meet the 90 minute fire resistance requirement for some structural parts. Google's controls to mitigate the risk of damage, loss, and outage of operations, are a combination of physical and logical controls. These controls include monitoring of temperature, humidity and smoke and the deployment of fire extinguishers/ other means of fire suppression at all in scope facilities. These facility controls, combined with Cloud's highly redundant architecture and geographically dispersed network, address the associated control objective. Management believes that this one criterion poses a low risk to customer workloads.

bernard@botmaker.io

Internal Google Traffic

Connections between internal Google resources use proprietary services similar to Remote Procedural Calls (RPC) that provide peer-to-peer authentication similar to Kerberos. All traffic is at least cryptographically authenticated between machines, while some connections, including to and from the Key Management Service, are encrypted using AES.

Key Management

Google uses a proprietary service to manage the distribution, generation and rotation of cryptographic keys. Files or data structures with user-generated content written by Cloud or App Engine services are encrypted with a key. This key is encrypted by the Key Management Service with a restricted access control list (ACL) of services allowed to request the Key Management Service to decrypt it. The encrypted key is not stored alongside the encrypted data.

The wrapping keys needed to decrypt user data are only known to the Key Management Service. All access to/from the Key Management Service is controlled by ACLs. Access is restricted to a limited number of individuals and applications, and auditing is enabled to determine whether access is appropriate.

Key Rotations

Google uses a proprietary system to periodically generate and rotate an encryption key used to protect user data at rest on average at least every 90 days. New wrapped encryption keys are generated for each new Google storage file (a Google file is defined in Encryption of Data Stored at Google above). The system helps ensure that key rotations are managed appropriately, and that customer data is not encrypted with a discarded key.

Disk Erase Process

Google has a policy stating that no loose drive may leave Google data centers unless it has been erased (or destroyed), certified as erased by Google, and validated as such by Google via audit. One or more types of disk erase mechanisms are used to delete data off disks before they are decommissioned. Multiple checks are performed to help ensure that all drives are accounted for. Non-erased loose drives are stored in a secure container until they are erased. The disk erase process is well defined, and each facility is audited on a daily basis to monitor compliance with the disk erase policy.

If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

bernard@bernaki.io

Docusign Envelope ID: 269130C8-431E-4611-B5B2-D2CDAEFEEEE7

Certificate

Certificate number: 2023-014

Certified by EY CertifyPoint since: August 25, 2023

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Google LLC*

located in Mountain View, California, United States of America is compliant with the requirements as stated in the standard:

CSA STAR CCM v.4

Issue date of certificate: May 10, 2024
Re-issue date of certificate: July 18, 2025
Expiration date of certificate: May 14, 2027
Last certification cycle expiration date: May 14, 2024

EY CertifyPoint will, according to the certification agreement dated May 23, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above. This certificate is only valid in combination with a valid and accredited ISO/IEC 27001:2022 certification with certificate number 2012-001b issued by EY CertifyPoint, last re-issued on June 30, 2025, with expiry date May 14, 2027.

**The certification is applicable for the assets, services and locations as described in the scoping section at the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, dated January 10, 2025.*

DocuSigned by:
Jatin Sehgal
3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V., located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Docusign Envelope ID: 269130C8-431E-4611-B5B2-D2CDAEFEEEE7

Google LLC

Scope for certificate 2023-014

The scope of this CSA STAR CCM v.4 certification is limited to the Google Cloud ISMS, which is implemented in the following product area, its offering(s) and locations as listed below, along with the data contained or collected by those offering(s). Moreover, the scope of this CSA STAR CCM v.4 certification is limited to Enterprise Customers.

Google Cloud Platform:

- Access Approval
- Access Context Manager
- Access Transparency
- Advanced API Security
- Agent Assist
- AI Platform Deep Learning Container
- AlloyDB
- Anti-Money Laundering AI
- API Gateway
- Apigee
- App Engine
- Application Integration
- Artifact Analysis
- Artifact Registry
- Assured Workloads
- AutoML Tables
- AutoML Translation
- Backup for GKE
- Batch
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- Certificate Authority Service
- Certificate Manager
- Chrome Enterprise Premium
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Billing
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Console
- Cloud Console App
- Cloud Data Fusion
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud External Key Manager (Cloud EKM)
- Cloud Filestore
- Cloud Functions
- Cloud Functions for Firebase
- Cloud Healthcare
- Cloud HSM
- Cloud IDS (Cloud Intrusion Detection System)
- Cloud Interconnect
- Cloud Key Management Service
- Cloud Life Sciences
- Cloud Load Balancing
- Cloud Logging
- Cloud Monitoring
- Cloud NAT (Network Address Translation)
- Cloud Natural Language API
- Cloud NGFW
- Cloud Org Policy
- Cloud Profiler
- Cloud Router
- Cloud Run
- Cloud Scheduler
- Cloud Service Mesh
- Cloud Shell
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speaker ID
- Cloud SQL
- Cloud Storage
- Cloud Storage for Firebase
- Cloud Tasks
- Cloud Trace
- Cloud Translation
- Cloud Vision

This scope is only valid in connection with certificate 2023-014.

Docusign Envelope ID: 269130C8-431E-4611-B5B2-D2CDAEFEEEE7

Google LLC

Scope for certificate 2023-014

Google Cloud Platform (continued):

- Cloud VPN
- Cloud Workstations
- Compute Engine
- Connect
- Container Registry
- Conversational AI
- Conversational Insights
- Data Catalog
- Database Migration Service
- Dataflow
- Dataform
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- Datastream
- Dialogflow
- Document AI
- Document AI Warehouse
- Eventarc
- Firebase App Check
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Food Ordering AI Agent
- Gemini for Google Cloud
- Generative AI on Vertex AI
- GKE Enterprise Config Management
- GKE Identity Service
- Google Cloud Armor
- Google Cloud Backup and DR
- Google Cloud Contact Center as a Service (CCaaS)
- Google Cloud Deploy
- Google Cloud Identity-Aware Proxy
- Google Cloud Marketplace
- Google Cloud SDK
- Google Cloud Skills Boost
- Google Earth Engine
- Google Kubernetes Engine
- Google Security Operations (SIEM)
- Google Security Operations (SOAR)
- Google Threat Intelligence
- GTI for Google Security Operations
- Healthcare Data Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- Infrastructure Manager
- Integration Connectors
- Key Access Justifications (KAJ)
- Knative serving
- Looker (Google Cloud core)
- Looker Studio
- Managed Service for Apache Kafka
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Migrate to Virtual Machines
- Migration Center
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- Parallelstore
- Persistent Disk
- Personalized Service Health
- Privileged Access Manager
- Pub/Sub
- Ray on Vertex
- reCAPTCHA Enterprise
- Recommendations AI
- Recommender
- Resource Manager API
- Retail Search
- Risk Manager
- SecLM
- Secret Manager
- Secure Source Manager

Docusign Envelope ID: 269130C8-431E-4611-B5B2-D2CDAEFEEEE7

Google LLC

Scope for certificate 2023-014

Google Cloud Platform (continued):

- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- Service Directory
- Service Infrastructure
- Service Mesh
- Spectrum Access System
- Speech-to-Text
- Storage Transfer Service
- Tables
- Talent Solution
- Text-to-Speech
- Traffic Director
- Transcoder API
- Vertex AI Colab Enterprise
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Vertex AI Workbench Instances
- Video Intelligence API
- Virtual Private Cloud
- VirusTotal
- VPC Service Controls
- Web Risk API
- Workflows
- Workload Manager

GCP Cloud Edge:

- Media CDN

Google Cloud Platform (GCP) Multi-Cloud Services:

- BigQuery Omni

Google Cloud NetApp Volumes (GCNV):

- Google Cloud NetApp Volumes

Google Cloud VMware Engine (GCVE):

- Google Cloud VMware Engine

The following locations are in scope:

Data Centers:

- Dammam, Saudi Arabia
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar

Docusign Envelope ID: 269130C8-431E-4611-B5B2-D2CDAEFEEEE7

Google LLC

Scope for certificate 2023-014

The ISMS is centrally managed out of the Google LLC headquarters in Mountain View, California, United States of America. The ISMS mentioned in the above scope is restricted as defined in 'Google Cloud Platform Scoping Document for CSA STAR CCM v4.0 Certification', reviewed on January 21, 2025, by the Cloud Core Certifications Lead.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

PBHVA cloud security assessment summary report Google Cloud Platform

This information technology security summary of the public Google Cloud Platform (Google) Software Services is an UNCLASSIFIED publication, issued under the authority of the Head, Canadian Centre for Cyber Security (Cyber Centre). To obtain a full copy of this Security Assessment, contact the Cyber Centre's Contact Centre at: Centre:

- by email: contact@cyber.gc.ca
- by phone: 613-949-7048 or 1-833-CYBER-88

This document is the property of the Government of Canada (GC), and it is not to be altered without the express permission of Cyber Centre. It may be distributed in whole to any interested party.

January 2025

© His Majesty the King in Right of Canada, as represented by the Minister of National Defence, 2025

Canada

General assessment information

Vendor Name	Google
Third-Party Assessment Organization (3PAO)	Coalfire Systems, Inc https://marketplace.fedramp.gov/assessors/138514
Assessment Conducted By	Canadian Centre for Cyber Security (Cyber Centre)
Assessment Completion Date	January 31, 2025
Data Categorization Level	PBHVA
Service Model	Software-as-a-service (SaaS)/infrastructure-as-a-service (IaaS)/platform-as-a-service (PaaS)
Hosted Provider (CSP)	IaaS Provider

Assessed services

Vendor Category	Services
AI and Machine Learning	• AI Platform Data Labeling • AI Platform Neural Architecture Search • AI Platform Training and Prediction • AutoML Natural Language • AutoML Tables • AutoML Translation • AutoML Video • AutoML Vision • Contact Center AI • Dialogflow • Document AI • Notebooks (formerly Vertex AI Workbench/AI Platform Notebooks) • Text-to-Speech • Vertex AI Forecast • Vertex AI Model Registry • Vertex ML Metadata • Vertex Model Monitoring

Vendor Category	Services
	• Vertex Online and Batch Prediction • Vertex Pipelines • Vertex Training
Analytics and Big Data	• BigQuery • BigQuery Data Transfer Service • Cloud Bigtable
Compute	• Cloud Functions • Cloud Run (fully managed) • Cloud Run for Anthos
Containers	• Apigee • App Engine • Cloud Build • Compute Engine • Container Registry • GKE Hub • Google Kubernetes Engine • VM Manager
Database	• Cloud Data Fusion • Cloud Functions for Firebase • Cloud SQL • Data Catalog • Database Migration Service • Datastore • DataStream • Memorystore
Developer Tools	• Cloud Composer • Cloud SDK • Cloud Shell • Cloud Source Repositories • Cloud Translation • Cloud Vision

Vendor Category	Services
	• Cloud Workstations • Dataflow • Eventarc
Metrics/Observability	• Anthos Config Management (ACM) • Anthos Service Mesh • Artifact Registry • Cloud Asset Inventory • Cloud Billing • Cloud Deployment Manager • Cloud Endpoints • Cloud Logging • Cloud Monitoring • Cloud Profiler • Cloud Scheduler • Cloud Tasks • Cloud Trace • Insights • Looker Studio (including Pro, formerly Google Data Studio) • Traffic Director
Network	• Cloud CDN • Cloud DNS • Cloud Interconnect • Cloud Load Balancing • Cloud NAT (Network address Translation) • Cloud Router • Cloud VPN • Google Cloud Armor • Network Connectivity Center • Network Intelligence Center • Network Service Tiers • Virtual Private Cloud (VPC) • VPC Service Controls
Security and Identity	• Access Approval • Access Context Manager • Access Transparency • Admin Console (incl. Admin SDK,Directory Sync)

Vendor Category	Services
	• Anthos Identity Service (AIS) • Assured Workloads • BeyondCorp Enterprise (note: split from Cloud Console) • Binary Authorization • Certificate Authority Service • Chronicle (Security Product) • Chronicle SOAR • Cloud Console (without BeyondCorp Enterprise) • Cloud Console App • Cloud Data Loss Prevention • Cloud External Key Manager (Cloud EKM) • Cloud HSM • Cloud IDS • Cloud Identity • Cloud Identity-Aware Proxy • Cloud Key Management Service • Connect • Firebase Authentication • Identity & Access Management • Identity Platform • Key Access Justification (Access Sovereignty) • reCAPTCHA Enterprise • Secret Manager • Security Command Center - Including Web Security Scanner (formerly Cloud Security Scanner) • Service Directory • Service Infrastructure (formerly Service Control; includes Service Management API and Service Consumer Management API) • Workforce Identity Federation (BYOID)
Storage	• Cloud Filestore • Cloud Spanner • Cloud Storage • Cloud Storage for Firebase • Firestore • Persistent Disk • Storage Transfer Service
Other	• Care Studio (formerly Cloud Healthcare Search)

Vendor Category	Services
	• Cloud Healthcare • Cloud Healthcare API • Cloud Life Sciences (formerly Google Genomics) • Cloud Natural Language API • Dataproc • Earth Engine • GCP Marketplace (formerly Cloud Launcher) • Pub/Sub • Resource Manager API • Speech-to-Text • Talent Solutions • Video Intelligence API • Web Risk API • Workflows

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Security assessment summary report

Google Cloud Platform

This information technology security summary of the public Google Cloud Platform (Google) Software Services is an UNCLASSIFIED publication, issued under the authority of the Head, Canadian Centre for Cyber Security (Cyber Centre). To obtain a full copy of this Security Assessment, contact the Cyber Centre's Contact Centre at:

Contact Centre
contact@cyber.gc.ca
613-949-7048
Toll Free: 1-833-CYBER-88

This document is the property of the Government of Canada (GC), and it is not to be altered without the express permission of Cyber Centre. It may be distributed in whole to any interested party.

May 2025

© His Majesty the King in Right of Canada, as represented by the Minister of National Defence, 2025

Canada

General assessment information

Vendor name	Google
Third-party assessment organization (3PAO)	Coalfire Systems, Inc. (https://marketplace.fedramp.gov/assessors/138514)
Assessment conducted by	Canadian Centre for Cyber Security (Cyber Centre)
Assessment completion date	May 30, 2025
Data categorization level	PBMM
Service model	Software-as-a-service (SaaS)/infrastructure-as-a-service (IaaS)/platform-as-a-service (PaaS)
Hosted provider (CSP)	IaaS provider

Assessed services

Vendor category	Services
Artificial intelligence (AI) and Machine learning (ML)	• AI platform data labelling • AI Platform Neural Architecture Search • AI Platform Training and Prediction • AutoML Natural Language • AutoML Tables • AutoML Translation • AutoML Video • AutoML Vision • Contact Center AI • Dialogflow • Document AI • Generative AI on Vertex AI • Notebooks (formerly Vertex AI Workbench/AI Platform Notebooks) • Text-to-Speech • Vertex AI Forecast • Vertex AI Model Registry • Vertex AI Search (includes Agentspace) • Vertex ML Metadata

Vendor category	Services
	• Vertex Model Monitoring • Vertex Online and Batch Prediction • Vertex Pipelines • Vertex Training
Analytics and big data	• BigQuery • BigQuery Data Transfer Service • Cloud Bigtable
Compute	• Cloud Functions • Cloud Run (fully managed) • Cloud Run for Anthos
Containers	• Apigee* • App Engine • Cloud Build • Compute Engine • Container Registry • GKE Hub • Google Kubernetes Engine • VM Manager
Database	• Cloud Data Fusion • Cloud Functions for Firebase • Cloud SQL • Data Catalog • Database Migration Service • Datastore • DataStream • Memorystore
Developer tools	• Cloud Composer • Cloud SDK • Cloud Shell • Cloud Source Repositories • Cloud Translation • Cloud Vision • Cloud Workstations • Dataflow • Eventarc

Vendor category	Services
Metrics/observability	• Anthos Config Management (ACM) • Anthos Service Mesh • Artifact Registry • Cloud Asset Inventory • Cloud Billing • Cloud Deployment Manager • Cloud Endpoints • Cloud Logging* • Cloud Monitoring* • Cloud Profiler* • Cloud Scheduler • Cloud Tasks • Cloud Trace* • Insights • Looker Studio (including Pro, formerly Google Data Studio)* • Traffic Director
Network	• Cloud CDN • Cloud DNS • Cloud Interconnect • Cloud Load Balancing • Cloud NAT (Network address Translation) • Cloud Router • Cloud VPN • Google Cloud Armor • Network Connectivity Center • Network Intelligence Center • Network Service Tiers • Virtual Private Cloud (VPC) • VPC Service Controls
Security and identity	• Access Approval • Access Context Manager • Access Transparency • Admin Console (incl. Admin SDK, Directory Sync) • Anthos Identity Service (AIS) • Assured Workloads • BeyondCorp Enterprise (note: split from Cloud Console)

Vendor category	Services
	• Binary Authorization • Certificate Authority Service • Chronicle (Security Product) • Chronicle SOAR • Cloud Console (without BeyondCorp Enterprise) • Cloud Console App • Cloud Data Loss Prevention • Cloud External Key Manager (Cloud EKM) • Cloud HSM • Cloud Identity • Cloud Identity-Aware Proxy • Cloud IDS • Cloud Key Management Service • Connect • Firebase Authentication • Identity & Access Management • Identity Platform • Key Access Justification (Access Sovereignty) • reCAPTCHA Enterprise • Secret Manager • Security Command Center - Including Web Security Scanner (formerly Cloud Security Scanner) • Service Directory • Service Infrastructure (formerly Service Control; includes Service Management API and Service Consumer Management API) • Workforce Identity Federation (BYOID)
Storage	• Cloud Filestore • Cloud Spanner • Cloud Storage • Cloud Storage for Firebase • Firestore • Persistent Disk • Storage Transfer Service
Google Workspace	• Classroom* • Cloud Search* • Gemini for Google Workspace* • Gmail*

Vendor category	Services
	• Gmail REST API* • Google Calendar* • Google Calendar API* • Google Chat* • Google Contacts* • Google Docs* • Google Drive* • Google Drive Activity API* • Google Drive REST API* • Google Forms* • Google Groups* • Google Jamboard* • Google Keep* • Google Meet* • Google Mobile Device Management* • Google People API* • Google Sheets* • Google Sheets API* • Google Sites* • Google Slides* • Google Tasks* • Google Tasks API* • Google Vault* • Google Vids* • Google Voice* • Google Workspace Migrate*
Other	• Care Studio (formerly Cloud Healthcare Search) • Cloud Healthcare • Cloud Healthcare API • Cloud Life Sciences (formerly Google Genomics) • Cloud Natural Language API • Dataproc • Earth Engine • GCP Marketplace (formerly Cloud Launcher) • Pub/Sub • Resource Manager API • Speech-to-Text

Vendor category	Services
	• Talent Solutions • Video Intelligence API • Web Risk API • Workflows

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Certificate

Certificate number: 2012-001b

Certified by EY CertifyPoint since: May 11, 2012

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Google LLC*

located in Mountain View, California, United States of America is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2022

Issue date of certificate: May 10, 2024
Re-issue date of certificate: September 22, 2025
Expiration date of certificate: May 14, 2027
Last certification cycle expiration date: May 14, 2024

EY CertifyPoint will, according to the certification agreement dated May 23, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

**The certification is applicable for the assets, services and locations as described in the scoping section at the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, dated May 22, 2025.*

DocuSigned by:
Jatin Sehgal
3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V, located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

The scope of this ISO/IEC 27001:2022 certification is limited to the Google Cloud ISMS, which is implemented in the following product area, its offering(s) and locations as listed below, along with the data contained or collected by those offering(s). Moreover, the scope of this ISO/IEC 27001:2022 certification is limited to Enterprise Customers.

Google Cloud Platform:

- Access Approval
- Access Context Manager
- Access Transparency
- Advanced API Security
- Agent Assist
- Agentspace
- AI Platform Deep Learning Container
- AlloyDB
- Anti-Money Laundering AI
- API Gateway
- Apigee
- App Engine
- Application Integration
- Artifact Analysis
- Artifact Registry
- Assured Workloads
- AutoML Tables
- AutoML Translation
- Backup for GKE
- Batch
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- Certificate Authority Service
- Certificate Manager
- Chrome Enterprise Premium
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Billing
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Console
- Cloud Console App
- Cloud Data Fusion
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud External Key Manager (Cloud EKM)
- Cloud Filestore
- Cloud Functions
- Cloud Functions for Firebase
- Cloud Healthcare
- Cloud HSM
- Cloud IDS (Cloud Intrusion Detection System)
- Cloud Interconnect
- Cloud Key Management Service
- Cloud Life Sciences
- Cloud Load Balancing
- Cloud Logging
- Cloud Monitoring
- Cloud NAT (Network Address Translation)
- Cloud Natural Language API
- Cloud NGFW
- Cloud Org Policy
- Cloud Profiler
- Cloud Router
- Cloud Run
- Cloud Scheduler
- Cloud Service Mesh
- Cloud Shell
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speaker ID
- Cloud SQL
- Cloud Storage
- Cloud Storage for Firebase
- Cloud Tasks
- Cloud Trace
- Cloud Translation

This scope is only valid in connection with certificate 2012-001b.

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

Google Cloud Platform (continued):

- Cloud Vision
- Cloud VPN
- Cloud Workstations
- Compute Engine
- Connect
- Container Registry
- Conversational AI
- Conversational Insights
- Data Catalog
- Database Migration Service
- Dataflow
- Dataform
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- Datastream
- Dialogflow
- Document AI
- Document AI Warehouse
- Eventarc
- Firebase App Check
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Food Ordering AI Agent
- Gemini Code Assist
- Gemini for Google Cloud
- Gemini in BigQuery
- Generative AI on Vertex AI
- GKE Enterprise Config Management
- GKE Identity Service
- Google Cloud Armor
- Google Cloud Backup and DR
- Google Cloud Contact Center as a Service (CCaaS)
- Google Cloud Deploy
- Google Cloud Identity-Aware Proxy
- Google Cloud Marketplace
- Google Cloud SDK
- Google Cloud Skills Boost
- Google Earth Engine
- Google Kubernetes Engine
- Google Public DNS
- Google Security Operations (SIEM)
- Google Security Operations (SOAR)
- Google Threat Intelligence
- GTI for Google Security Operations
- Healthcare Data Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- Infrastructure Manager
- Integration Connectors
- Key Access Justifications (KAJ)
- Knative serving
- Looker (Google Cloud core)
- Looker Studio
- Managed Service for Apache Kafka
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Migrate to Virtual Machines
- Migration Center
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- NotebookLM for enterprise
- Parallelstore
- Persistent Disk
- Personalized Service Health
- Privileged Access Manager
- Pub/Sub
- reCAPTCHA Enterprise
- Ray on Vertex
- Recommendations AI
- Recommender
- Resource Manager API

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

Google Cloud Platform (continued):

- Retail Search
- Risk Manager
- SecLM
- Secret Manager
- Secure Source Manager
- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- Service Directory
- Service Infrastructure
- Service Mesh
- Spectrum Access System
- Speech-to-Text
- Storage Transfer Service
- Tables
- Talent Solution
- Text-to-Speech
- Traffic Director
- Transcoder API
- Transfer Appliance
- Vertex AI Colab Enterprise
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Vertex AI Workbench Instances
- Video Intelligence API
- Virtual Private Cloud
- VirusTotal
- VPC Service Controls
- Web Risk API
- Workflows
- Workload Manager

Google Cloud Platform (GCP) Bare Metal (Rack) HSM:

- Bare Metal HSM
- Bare Metal Rack HSM

Google Cloud Platform (GCP) Cloud Edge:

- Google Distributed Cloud connected
- Media CDN

Google Cloud Platform (GCP) Cloud Software:

- Binary Authorization – Software
- Cloud Monitoring – Software
- Connect – Software
- GKE Enterprise Config Management - Software
- GKE Identity Service – Software
- GKE on AWS
- GKE on Azure
- Google Distributed Cloud Hosted (GDCH) – Software
- Google Distributed Cloud Virtual (GDCV) for Bare Metal
- Google Distributed Cloud Virtual (GDCV) for VMware
- Knative serving – Software
- Migrate to Containers
- Network Gateway for Google Distributed Cloud
- Service Mesh – Software
- Speech-to-Text On-Prem
- Telecom Subscriber Insights

Google Cloud Platform (GCP) Multi-Cloud Services:

- BigQuery Omni

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

Google Cloud NetApp Volumes (GCNV):

- Google Cloud NetApp Volumes

Google Cloud VMware Engine (GCVE):

- Google Cloud VMware Engine

The following locations are in scope:

Data Centers:

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Austin (TX), United States of America
- Berlin (1), Germany
- Berlin (2), Germany
- Berlin (3), Germany
- Chandler (AZ), United States of America
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Dalarna, Sweden
- Dammam, Saudi Arabia
- Dammam (2), Saudi Arabia
- Dammam (3), Saudi Arabia
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India
- Delhi (4), India
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Frankfurt (9), Hesse, Germany
- Fredericia, Denmark
- Gainesville (VA), United States of America
- Ghlin, Hainaut, Belgium
- Guanajuato, Mexico
- Hamina, Finland
- Henderson (NV), United States of America
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia
- Johannesburg (1), South Africa

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

Data Centers (continued):

- Johannesburg (2), South Africa
- Johannesburg (3), South Africa
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Las Vegas (NV), United States of America
- Lancaster (OH), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Lok Yang Way, Singapore
- London (1), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Loyang, Singapore
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Markham, Ontario, Canada
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia
- Middenmeer, Noord-Holland, the Netherlands
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America
- Midlothian (3) (TX), United States of America
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada
- Montreal (2), Quebec, Canada
- Mumbai (1), India
- Mumbai (2), India
- Mumbai (3), India
- Mumbai (4), India
- Mumbai (5), India
- New Albany (OH), United States of America
- Omaha (NE), United States of America
- Osaka (1), Japan
- Osaka (2), Japan
- Osasco, Brazil
- Papillion (NE), United States of America
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Phoenix (AZ), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile
- Quilicura (3), Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- San Bernardo, Santiago, Chile
- Santana de Parnaíba, Brazil
- Seoul (1), South Korea
- Seoul (2), South Korea

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

Data Centers (continued):

- Seoul (3), South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- The Dalles (3) (OR), United States of America
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Vinhedo, Brazil
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Wenya, Singapore
- Widows Creek (AL), United States of America
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland

Offices:

- Accra, Ghana
- Addison (TX), United States of America
- Amsterdam, The Netherlands
- Ann Arbor (MI), United States of America
- Athens, Greece
- Atlanta (GA), United States of America
- Auckland, New Zealand
- Austin (TX), United States of America
- Bangalore, India
- Bangkok, Thailand
- Barcelona, Spain
- Beijing, China
- Bellevue (WA), United States of America
- Belo Horizonte, Brazil
- Berlin, Germany
- Bogota, Colombia
- Boston (MA), United States of America
- Bothell (WA), United States of America
- Boulder (CO), United States of America
- Brisbane, Australia
- Brussels, Belgium
- Bucharest, Romania
- Budapest, Hungary
- Buenos Aires, Argentina
- Cairo, Egypt
- Calgary, Alberta, Canada
- Cambridge (MA), United States of America
- Cebu City, Philippines
- Charlotte (NC), United States of America
- Chicago (IL), United States of America
- Copenhagen, Denmark
- Detroit (MI), United States of America
- Doha, Qatar
- Dubai, United Arab Emirates
- Dublin, Ireland
- Durham (NC), United States of America

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

Offices (continued):

- Espoo, Finland
- Frankfurt, Germany
- Fremont (CA), United States of America
- Gandhinagar, India
- Gdansk, Poland
- Goleta (CA), United States of America
- Ghent, Belgium
- Gurgaon, India
- Haifa, Israel
- Hamburg, Germany
- Hanoi, Vietnam
- Helsinki, Finland
- Hong Kong, Hong Kong
- Houston (TX), United States of America
- Hyderabad, India
- Irvine (CA), United States of America
- Istanbul, Turkey
- Johannesburg, South Africa
- Kirkland (WA), United States of America
- Kitchener, Canada
- Krakow, Poland
- Kuala Lumpur, Malaysia
- Lagos, Nigeria
- Lima, Peru
- Lisbon, Portugal
- London, United Kingdom
- Los Angeles (CA), United States of America
- Madison (WI), United States of America
- Madrid, Spain
- Malaga, Spain
- Manchester, United Kingdom
- Manila, Philippines
- Melbourne, Australia
- Mexico City, Mexico
- Miami (FL), United States of America
- Milan, Italy
- Montreal, Québec, Canada
- Mountain View (CA), United States of America
- Mumbai, India
- Munich, Germany
- Nairobi, Kenya
- Nashville (TN), United States of America
- New Taipei City, Taiwan
- New York (NY), United States of America
- Osaka, Japan
- Oslo, Norway
- Ottawa, Ontario, Canada
- Palo Alto (CA), United States of America
- Paris, France
- Perth, Australia
- Pittsburgh (PA), United States of America
- Playa Vista (CA), United States of America
- Portland (OR), United States of America
- Poughkeepsie (NY), United States of America
- Prague, Czech Republic
- Princeton (NJ), United States of America
- Pune, India
- Quezon City, Philippines
- Ramat Gan, Israel
- Redmond (WA), United States of America
- Redwood City (CA), United States of America
- Reston (VA), United States of America

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

Offices (continued):

- Riyadh, Saudi Arabia
- Rome, Italy
- Salt Lake City (UT), United States of America
- San Bruno (CA), United States of America
- San Diego (CA), United States of America
- San Francisco (CA), United States of America
- San Jose (CA), United States of America
- Santa Cruz (CA), United States of America
- Santiago, Chile
- Sao Paulo, Brazil
- Seattle (WA), United States of America
- Seoul, South Korea
- Shanghai, China
- Shenzhen, China
- Singapore, Singapore
- South Jakarta, Indonesia
- South San Francisco (CA), United States of America
- Southaven (MS), United States of America
- Stockholm, Sweden
- Sunnyvale (CA), United States of America
- Sydney, Australia
- Taipei, Taiwan
- Taoyuan, Taiwan
- Tel Aviv, Israel
- Thornton (CO), United States of America
- Tokyo, Japan
- Toronto, Canada
- Vancouver, Canada
- Viby, Denmark
- Vienna, Austria
- Vilnius, Lithuania
- Virginia (VA), United States of America
- Warsaw, Poland
- Washington, D.C., United States of America
- Wroclaw, Poland
- Zagreb, Croatia
- Zhubei City, Taiwan
- Zurich, Switzerland

The Information Security Management System is centrally managed out of the Google LLC headquarters in Mountain View, California, United States of America. The Information Security Management System mentioned in the above scope is restricted as defined in 'Google Cloud Services Information Security Management Implementation Manual', reviewed on May 22, 2025, by the Cloud Core Certifications Lead.

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2012-001b

Google LLC (including Google Cloud Platform) uses corporate entities as subsidiary companies to conduct business with its customers. The scope of the Information Security Management System includes the corporate entities listed below:

- Google Inc.
- Google Ireland Ltd ("GIL")
- Google Asia Pacific ("GAP")
- Google Cloud EMEA Ltd ("GCEMEA")
- Google Cloud Public Sector - United Kingdom ("GCPS-UK")
- Google Cloud Public Sector - Deutschland GmbH

Google LLC (Google Cloud) provides consulting services to its customers. The consulting team "Google Cloud Professional Services Organization" is included in the Google Cloud Information Security Management System.

As per the Statement of Applicability for the Google Cloud Information Security Management System, dated May 22, 2025, all 93 controls contained in Annex A of ISO/IEC 27001:2022 are in scope for this certification.

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Certificate

Certificate number: 2016-004b

Certified by EY CertifyPoint since: April 15, 2016

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Google LLC*

located in Mountain View, California, United States of America is compliant with the requirements as stated in the standard:

ISO/IEC 27017:2015

Issue date of certificate: May 10, 2024
Re-issue date of certificate: September 22, 2025
Expiration date of certificate: May 14, 2027
Last certification cycle expiration date: May 14, 2024

EY CertifyPoint will, according to the certification agreement dated May 23, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above or the expiration of the corresponding ISO/IEC 27001:2022 certification with certificate number 2012-001b.

**The certification is applicable for the assets, services and locations as described in the scoping section at the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, dated May 22, 2025.*

DocuSigned by:
Jatin Sehgal
3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V, located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-004b

The scope of this ISO/IEC 27017:2015 certification is limited to the Google Cloud ISMS, which is implemented in the following product area, its offering(s) and locations as listed below, along with the data contained or collected by those offering(s). Moreover, the scope of this ISO/IEC 27017:2015 certification is limited to Enterprise Customers.

Google Cloud Platform:

- Access Approval
- Access Context Manager
- Access Transparency
- Advanced API Security
- Agent Assist
- Agentspace
- AlloyDB
- Anti-Money Laundering AI
- API Gateway
- Apigee
- App Engine
- Application Integration
- Artifact Registry
- Assured Workloads
- AutoML Tables
- AutoML Translation
- Backup for GKE
- Batch
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- Certificate Authority Service
- Certificate Manager
- Chrome Enterprise Premium
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Billing
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Console
- Cloud Console App
- Cloud Data Fusion
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud External Key Manager (Cloud EKM)
- Cloud Filestore
- Cloud Functions
- Cloud Functions for Firebase
- Cloud Healthcare
- Cloud HSM
- Cloud IDS (Cloud Intrusion Detection System)
- Cloud Interconnect
- Cloud Key Management Service
- Cloud Life Sciences
- Cloud Load Balancing
- Cloud Logging
- Cloud Monitoring
- Cloud NAT (Network Address Translation)
- Cloud Natural Language API
- Cloud NGFW
- Cloud Org Policy
- Cloud Profiler
- Cloud Router
- Cloud Run
- Cloud Scheduler
- Cloud Service Mesh
- Cloud Shell
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speaker ID
- Cloud SQL
- Cloud Storage
- Cloud Storage for Firebase
- Cloud Tasks
- Cloud Trace
- Cloud Translation
- Cloud Vision

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-004b

Google Cloud Platform (continued):

- Cloud VPN
- Cloud Workstations
- Compute Engine
- Connect
- Container Registry
- Conversational AI
- Conversational Insights
- Data Catalog
- Database Migration Service
- Dataflow
- Dataform
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- Datastream
- Dialogflow
- Document AI
- Document AI Warehouse
- Eventarc
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Gemini Code Assist
- Gemini for Google Cloud
- Gemini in BigQuery
- Generative AI on Vertex AI
- GKE Enterprise Config Management
- GKE Identity Service
- Google Cloud Armor
- Google Cloud Backup and DR
- Google Cloud Contact Center as a Service (CCaaS)
- Google Cloud Deploy
- Google Cloud Identity-Aware Proxy
- Google Cloud Marketplace
- Google Cloud SDK
- Google Earth Engine
- Google Kubernetes Engine
- Google Security Operations (SIEM)
- Google Security Operations (SOAR)
- GTI for Google Security Operations
- Healthcare Data Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- Integration Connectors
- Key Access Justifications (KAJ)
- Knative serving
- Looker (Google Cloud core)
- Looker Studio
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Migrate to Virtual Machines
- Migration Center
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- NotebookLM for enterprise
- Persistent Disk
- Pub/Sub
- reCAPTCHA Enterprise
- Recommendations AI
- Recommender
- Resource Manager API
- Retail Search
- Risk Manager
- Secret Manager
- Secure Source Manager
- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- Service Directory
- Service Infrastructure
- Service Mesh
- Spectrum Access System
- Speech-to-Text

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-004b

Google Cloud Platform (continued):

- Storage Transfer Service
- Talent Solution
- Text-to-Speech
- Traffic Director
- Transcoder API
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Video Intelligence API
- Virtual Private Cloud
- VPC Service Controls
- Web Risk API
- Workflows
- Workload Manager

Google Cloud Platform (GCP) Multi-Cloud Services:

- BigQuery Omni

Google Cloud Platform (GCP) Cloud Edge:

- Media CDN

Google Cloud NetApp Volumes (GCNV):

- Google Cloud NetApp Volumes

Google Cloud VMWare Engine (GCVE):

- Google Cloud VMWare Engine

The following locations are in scope:

Data Centers:

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Austin (TX), United States of America
- Berlin (1), Germany
- Berlin (2), Germany
- Berlin (3), Germany
- Chandler (AZ), United States of America
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Dalarna, Sweden
- Dammam, Saudi Arabia
- Dammam (2), Saudi Arabia
- Dammam (3), Saudi Arabia
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-004b

Data Centers (continued):

- Delhi (4), India
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Frankfurt (9), Hesse, Germany
- Fredericia, Denmark
- Gainesville (VA), United States of America
- Ghlin, Hainaut, Belgium
- Guanajuato, Mexico
- Hamina, Finland
- Henderson (NV), United States of America
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia
- Johannesburg (1), South Africa
- Johannesburg (2), South Africa
- Johannesburg (3), South Africa
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Las Vegas (NV), United States of America
- Lancaster (OH), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Lok Yang Way, Singapore
- London (1), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Loyang, Singapore
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Markham, Ontario, Canada
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia
- Middenmeer, Noord-Holland, the Netherlands
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America
- Midlothian (3) (TX), United States of America
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada
- Montreal (2), Quebec, Canada
- Mumbai (1), India
- Mumbai (2), India
- Mumbai (3), India

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-004b

Data Centers (continued):

- Mumbai (4), India
- Mumbai (5), India
- New Albany (OH), United States of America
- Omaha (NE), United States of America
- Osaka (1), Japan
- Osaka (2), Japan
- Osasco, Brazil
- Papillion (NE), United States of America
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Phoenix (AZ), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile
- Quilicura (3), Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- San Bernardo, Santiago, Chile
- Santana de Parnaíba, Brazil
- Seoul (1), South Korea
- Seoul (2), South Korea
- Seoul (3), South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- The Dalles (3) (OR), United States of America
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Vinhedo, Brazil
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Wenya, Singapore
- Widows Creek (AL), United States of America
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland

Offices:

- Accra, Ghana
- Addison (TX), United States of America
- Amsterdam, The Netherlands
- Ann Arbor (MI), United States of America
- Athens, Greece
- Atlanta (GA), United States of America
- Auckland, New Zealand
- Austin (TX), United States of America
- Bangalore, India
- Bangkok, Thailand

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-004b

Offices (continued):

- Barcelona, Spain
- Beijing, China
- Bellevue (WA), United States of America
- Belo Horizonte, Brazil
- Berlin, Germany
- Bogota, Colombia
- Boston (MA), United States of America
- Bothell (WA), United States of America
- Boulder (CO), United States of America
- Brisbane, Australia
- Brussels, Belgium
- Bucharest, Romania
- Budapest, Hungary
- Buenos Aires, Argentina
- Cairo, Egypt
- Calgary, Alberta, Canada
- Cambridge (MA), United States of America
- Cebu City, Philippines
- Charlotte (NC), United States of America
- Chicago (IL), United States of America
- Copenhagen, Denmark
- Detroit (MI), United States of America
- Doha, Qatar
- Dubai, United Arab Emirates
- Dublin, Ireland
- Durham (NC), United States of America
- Espoo, Finland
- Frankfurt, Germany
- Fremont (CA), United States of America
- Gandhinagar, India
- Gdansk, Poland
- Goleta (CA), United States of America
- Ghent, Belgium
- Gurgaon, India
- Haifa, Israel
- Hamburg, Germany
- Hanoi, Vietnam
- Helsinki, Finland
- Hong Kong, Hong Kong
- Houston (TX), United States of America
- Hyderabad, India
- Irvine (CA), United States of America
- Istanbul, Turkey
- Johannesburg, South Africa
- Kirkland (WA), United States of America
- Kitchener, Canada
- Krakow, Poland
- Kuala Lumpur, Malaysia
- Lagos, Nigeria
- Lima, Peru
- Lisbon, Portugal
- London, United Kingdom
- Los Angeles (CA), United States of America
- Madison (WI), United States of America
- Madrid, Spain
- Malaga, Spain
- Manchester, United Kingdom
- Manila, Philippines
- Melbourne, Australia
- Mexico City, Mexico
- Miami (FL), United States of America
- Milan, Italy
- Montreal, Québec, Canada
- Mountain View (CA), United States of America

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-004b

Offices (continued):

- Mumbai, India
- Munich, Germany
- Nairobi, Kenya
- Nashville (TN), United States of America
- New Taipei City, Taiwan
- New York (NY), United States of America
- Osaka, Japan
- Oslo, Norway
- Ottawa, Ontario, Canada
- Palo Alto (CA), United States of America
- Paris, France
- Perth, Australia
- Pittsburgh (PA), United States of America
- Playa Vista (CA), United States of America
- Portland (OR), United States of America
- Poughkeepsie (NY), United States of America
- Prague, Czech Republic
- Princeton (NJ), United States of America
- Pune, India
- Quezon City, Philippines
- Ramat Gan, Israel
- Redmond (WA), United States of America
- Redwood City (CA), United States of America
- Reston (VA), United States of America
- Riyadh, Saudi Arabia
- Rome, Italy
- Salt Lake City (UT), United States of America
- San Bruno (CA), United States of America
- San Diego (CA), United States of America
- San Francisco (CA), United States of America
- San Jose (CA), United States of America
- Santa Cruz (CA), United States of America
- Santiago, Chile
- Sao Paulo, Brazil
- Seattle (WA), United States of America
- Seoul, South Korea
- Shanghai, China
- Shenzhen, China
- Singapore, Singapore
- South Jakarta, Indonesia
- South San Francisco (CA), United States of America
- Southaven (MS), United States of America
- Stockholm, Sweden
- Sunnyvale (CA), United States of America
- Sydney, Australia
- Taipei, Taiwan
- Taoyuan, Taiwan
- Tel Aviv, Israel
- Thornton (CO), United States of America
- Tokyo, Japan
- Toronto, Canada
- Vancouver, Canada
- Viby, Denmark
- Vienna, Austria
- Vilnius, Lithuania
- Virginia (VA), United States of America
- Warsaw, Poland
- Washington, D.C., United States of America

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-004b

Offices (continued):

- Wroclaw, Poland
- Zagreb, Croatia
- Zhubei City, Taiwan
- Zurich, Switzerland

The Information Security Management System is centrally managed out of the Google LLC headquarters in Mountain View, California, United States of America. The Information Security Management System mentioned in the above scope is restricted as defined in 'Google Cloud Services Information Security Management Implementation Manual', reviewed on May 22, 2025, by the Cloud Core Certifications Lead.

Google LLC (including Google Cloud Platform) uses corporate entities as subsidiary companies to conduct business with its customers. The scope of the Information Security Management System includes the corporate entities listed below:

- Google Inc.
- Google Ireland Ltd ("GIL")
- Google Asia Pacific ("GAP")
- Google Cloud EMEA Ltd ("GCEMEA")
- Google Cloud Public Sector - United Kingdom ("GCPS-UK")
- Google Cloud Public Sector - Deutschland GmbH

Google LLC (Google Cloud) provides consulting services to its customers. The consulting team "Google Cloud Professional Services Organization" is included in the Google Cloud Information Security Management System.

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Certificate

Certificate number: 2016-005b

Certified by EY CertifyPoint since: April 15, 2016

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Google LLC*

located in Mountain View, California, United States of America is compliant with the requirements as stated in the standard:

ISO/IEC 27018:2019

Issue date of certificate: May 10, 2024
Re-issue date of certificate: September 22, 2025
Expiration date of certificate: May 14, 2027
Last certification cycle expiration date: May 14, 2024

EY CertifyPoint will, according to the certification agreement dated May 23, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above or the expiration of the corresponding ISO/IEC 27001:2022 certification with certificate number 2012-001b.

**The certification is applicable for the assets, services and locations as described in the scoping section at the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, dated May 22, 2025.*

DocuSigned by:
Jatin Sehgal
3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V, located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-005b

The scope of this ISO/IEC 27018:2019 certification is limited to the Google Cloud ISMS, which is implemented in the following product area, its offering(s) and locations as listed below, along with the data contained or collected by those offering(s). Moreover, the scope of this ISO/IEC 27018:2019 certification is limited to Enterprise Customers.

Google Cloud Platform:

- Access Approval
- Access Context Manager
- Access Transparency
- Advanced API Security
- Agent Assist
- Agentspace
- AlloyDB
- Anti-Money Laundering AI
- API Gateway
- Apigee
- App Engine
- Application Integration
- Artifact Registry
- Assured Workloads
- AutoML Tables
- AutoML Translation
- Backup for GKE
- Batch
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- Certificate Authority Service
- Certificate Manager
- Chrome Enterprise Premium
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Billing
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Console
- Cloud Console App
- Cloud Data Fusion
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud External Key Manager (Cloud EKM)
- Cloud Filestore
- Cloud Functions
- Cloud Functions for Firebase
- Cloud Healthcare
- Cloud HSM
- Cloud IDS (Cloud Intrusion Detection System)
- Cloud Interconnect
- Cloud Key Management Service
- Cloud Life Sciences
- Cloud Load Balancing
- Cloud Logging
- Cloud Monitoring
- Cloud NAT (Network Address Translation)
- Cloud Natural Language API
- Cloud NGFW
- Cloud Org Policy
- Cloud Profiler
- Cloud Router
- Cloud Run
- Cloud Scheduler
- Cloud Service Mesh
- Cloud Shell
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speaker ID
- Cloud SQL
- Cloud Storage
- Cloud Storage for Firebase
- Cloud Tasks
- Cloud Trace
- Cloud Translation
- Cloud Vision

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-005b

Google Cloud Platform (continued):

- Cloud VPN
- Cloud Workstations
- Compute Engine
- Connect
- Container Registry
- Conversational AI
- Conversational Insights
- Data Catalog
- Database Migration Service
- Dataflow
- Dataform
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- Datastream
- Dialogflow
- Document AI
- Document AI Warehouse
- Eventarc
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Gemini Code Assist
- Gemini for Google Cloud
- Gemini in BigQuery
- Generative AI on Vertex AI
- GKE Enterprise Config Management
- GKE Identity Service
- Google Cloud Armor
- Google Cloud Backup and DR
- Google Cloud Contact Center as a Service (CCaaS)
- Google Cloud Deploy
- Google Cloud Identity-Aware Proxy
- Google Cloud Marketplace
- Google Cloud SDK
- Google Earth Engine
- Google Kubernetes Engine
- Google Security Operations (SIEM)
- Google Security Operations (SOAR)
- GTI for Google Security Operations
- Healthcare Data Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- Integration Connectors
- Key Access Justifications (KAJ)
- Knative serving
- Looker (Google Cloud core)
- Looker Studio
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Migrate to Virtual Machines
- Migration Center
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- NotebookLM for enterprise
- Persistent Disk
- Pub/Sub
- reCAPTCHA Enterprise
- Recommendations AI
- Recommender
- Resource Manager API
- Retail Search
- Risk Manager
- Secret Manager
- Secure Source Manager
- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- Service Directory
- Service Infrastructure
- Service Mesh
- Spectrum Access System
- Speech-to-Text

This scope is only valid in connection with certificate 2016-005b.

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-005b

Google Cloud Platform (continued):

- Storage Transfer Service
- Talent Solution
- Text-to-Speech
- Traffic Director
- Transcoder API
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Video Intelligence API
- Virtual Private Cloud
- VPC Service Controls
- Web Risk API
- Workflows
- Workload Manager

Google Cloud Platform (GCP) Multi-Cloud Services:

- BigQuery Omni

Google Cloud Platform (GCP) Cloud Edge:

- Media CDN

Google Cloud NetApp Volumes (GCNV):

- Google Cloud NetApp Volumes

Google Cloud VMWare Engine (GCVE):

- Google Cloud VMWare Engine

The following locations are in scope:

Data Centers:

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Austin (TX), United States of America
- Berlin (1), Germany
- Berlin (2), Germany
- Berlin (3), Germany
- Chandler (AZ), United States of America
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Dalarna, Sweden
- Dammam, Saudi Arabia
- Dammam (2), Saudi Arabia
- Dammam (3), Saudi Arabia
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-005b

Data Centers (continued):

- Delhi (4), India
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Frankfurt (9), Hesse, Germany
- Fredericia, Denmark
- Gainesville (VA), United States of America
- Ghlin, Hainaut, Belgium
- Guanajuato, Mexico
- Hamina, Finland
- Henderson (NV), United States of America
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia
- Johannesburg (1), South Africa
- Johannesburg (2), South Africa
- Johannesburg (3), South Africa
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Las Vegas (NV), United States of America
- Lancaster (OH), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Lok Yang Way, Singapore
- London (1), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Loyang, Singapore
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Markham, Ontario, Canada
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia
- Middenmeer, Noord-Holland, the Netherlands
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America
- Midlothian (3) (TX), United States of America
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada
- Montreal (2), Quebec, Canada
- Mumbai (1), India
- Mumbai (2), India
- Mumbai (3), India
- Mumbai (4), India

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-005b

Data Centers (continued):

- Mumbai (5), India
- New Albany (OH), United States of America
- Omaha (NE), United States of America
- Osaka (1), Japan
- Osaka (2), Japan
- Osasco, Brazil
- Papillion (NE), United States of America
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Phoenix (AZ), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile
- Quilicura (3), Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- San Bernardo, Santiago, Chile
- Santana de Parnaíba, Brazil
- Seoul (1), South Korea
- Seoul (2), South Korea
- Seoul (3), South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- The Dalles (3) (OR), United States of America
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Vinhedo, Brazil
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Wenya, Singapore
- Widows Creek (AL), United States of America
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland

Offices:

- Accra, Ghana
- Addison (TX), United States of America
- Amsterdam, The Netherlands
- Ann Arbor (MI), United States of America
- Athens, Greece
- Atlanta (GA), United States of America
- Auckland, New Zealand
- Austin (TX), United States of America
- Bangalore, India
- Bangkok, Thailand
- Barcelona, Spain
- Beijing, China
- Bellevue (WA), United States of America

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-005b

Offices (continued):

- Belo Horizonte, Brazil
- Berlin, Germany
- Bogota, Colombia
- Boston (MA), United States of America
- Bothell (WA), United States of America
- Boulder (CO), United States of America
- Brisbane, Australia
- Brussels, Belgium
- Bucharest, Romania
- Budapest, Hungary
- Buenos Aires, Argentina
- Cairo, Egypt
- Calgary, Alberta, Canada
- Cambridge (MA), United States of America
- Cebu City, Philippines
- Charlotte (NC), United States of America
- Chicago (IL), United States of America
- Copenhagen, Denmark
- Detroit (MI), United States of America
- Doha, Qatar
- Dubai, United Arab Emirates
- Dublin, Ireland
- Durham (NC), United States of America
- Espoo, Finland
- Frankfurt, Germany
- Fremont (CA), United States of America
- Gandhinagar, India
- Gdansk, Poland
- Goleta (CA), United States of America
- Ghent, Belgium
- Gurgaon, India
- Haifa, Israel
- Hamburg, Germany
- Hanoi, Vietnam
- Helsinki, Finland
- Hong Kong, Hong Kong
- Houston (TX), United States of America
- Hyderabad, India
- Irvine (CA), United States of America
- Istanbul, Turkey
- Johannesburg, South Africa
- Kirkland (WA), United States of America
- Kitchener, Canada
- Krakow, Poland
- Kuala Lumpur, Malaysia
- Lagos, Nigeria
- Lima, Peru
- Lisbon, Portugal
- London, United Kingdom
- Los Angeles (CA), United States of America
- Madison (WI), United States of America
- Madrid, Spain
- Malaga, Spain
- Manchester, United Kingdom
- Manila, Philippines
- Melbourne, Australia
- Mexico City, Mexico
- Miami (FL), United States of America
- Milan, Italy
- Montreal, Québec, Canada
- Mountain View (CA), United States of America
- Mumbai, India
- Munich, Germany
- Nairobi, Kenya
- Nashville (TN), United States of America
- New Taipei City, Taiwan

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-005b

Offices (continued):

- New York (NY), United States of America
- Osaka, Japan
- Oslo, Norway
- Ottawa, Ontario, Canada
- Palo Alto (CA), United States of America
- Paris, France
- Perth, Australia
- Pittsburgh (PA), United States of America
- Playa Vista (CA), United States of America
- Portland (OR), United States of America
- Poughkeepsie (NY), United States of America
- Prague, Czech Republic
- Princeton (NJ), United States of America
- Pune, India
- Quezon City, Philippines
- Ramat Gan, Israel
- Redmond (WA), United States of America
- Redwood City (CA), United States of America
- Reston (VA), United States of America
- Riyadh, Saudi Arabia
- Rome, Italy
- Salt Lake City (UT), United States of America
- San Bruno (CA), United States of America
- San Diego (CA), United States of America
- San Francisco (CA), United States of America
- San Jose (CA), United States of America
- Santa Cruz (CA), United States of America
- Santiago, Chile
- Sao Paulo, Brazil
- Seattle (WA), United States of America
- Seoul, South Korea
- Shanghai, China
- Shenzhen, China
- Singapore, Singapore
- South Jakarta, Indonesia
- South San Francisco (CA), United States of America
- Southaven (MS), United States of America
- Stockholm, Sweden
- Sunnyvale (CA), United States of America
- Sydney, Australia
- Taipei, Taiwan
- Taoyuan, Taiwan
- Tel Aviv, Israel
- Thornton (CO), United States of America
- Tokyo, Japan
- Toronto, Canada
- Vancouver, Canada
- Viby, Denmark
- Vienna, Austria
- Vilnius, Lithuania
- Virginia (VA), United States of America
- Warsaw, Poland
- Washington, D.C., United States of America
- Wroclaw, Poland
- Zagreb, Croatia
- Zhubei City, Taiwan
- Zurich, Switzerland

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2016-005b

The Information Security Management System is centrally managed out of the Google LLC headquarters in Mountain View, California, United States of America. The Information Security Management System mentioned in the above scope is restricted as defined in 'Google Cloud Services Information Security Management Implementation Manual', reviewed on May 22, 2025, by the Cloud Core Certifications Lead.

Google LLC (including Google Cloud Platform) uses corporate entities as subsidiary companies to conduct business with its customers. The scope of the Information Security Management System includes the corporate entities listed below:

- Google Inc.
- Google Ireland Ltd ("GIL")
- Google Asia Pacific ("GAP")
- Google Cloud EMEA Ltd ("GCEMEA")
- Google Cloud Public Sector - United Kingdom ("GCPS-UK")
- Google Cloud Public Sector - Deutschland GmbH

Google LLC (Google Cloud) provides consulting services to its customers. The consulting team "Google Cloud Professional Services Organization" is included in the Google Cloud Information Security Management System.

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Certificate

Certificate number: 2021-017

Certified by EY CertifyPoint since: May 14, 2021

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Privacy Information Management System as defined and implemented by

Google LLC*

located in Mountain View, California, United States of America is compliant with the requirements as stated in the standard:

ISO/IEC 27701:2019

Issue date of certificate: May 10, 2024
Re-issue date of certificate: September 22, 2025
Expiration date of certificate: May 14, 2027
Last certification cycle expiration date: May 14, 2024

EY CertifyPoint will, according to the certification agreement dated May 23, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above or the expiration of the corresponding ISO/IEC 27001:2022 certification with certificate number 2012-001b.

**The certification is applicable for the assets, services and locations as described in the scoping section at the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, dated May 23, 2025.*

DocuSigned by:
Jatin Sehgal
3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V, located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2021-017

The scope of this ISO/IEC 27701:2019 certification is limited to the Google Cloud PIMS, which is implemented in the following product area, its offering(s) and locations as listed below, along with the data contained or collected by those offering(s), applicable to Google LLC as PII processor for the PII processing activities within those offering(s). Moreover, the scope of this ISO/IEC 27701:2019 certification is limited to Enterprise Customers.

Google Cloud Platform:

- Access Approval
- Access Context Manager
- Access Transparency
- Advanced API Security
- Agent Assist
- Agentspace
- AlloyDB
- Anti-Money Laundering AI
- API Gateway
- Apigee
- App Engine
- Application Integration
- Artifact Registry
- Assured Workloads
- AutoML Tables
- AutoML Translation
- Backup for GKE
- Batch
- BigQuery
- BigQuery Data Transfer Service
- Binary Authorization
- Certificate Authority Service
- Certificate Manager
- Chrome Enterprise Premium
- Cloud Asset Inventory
- Cloud Bigtable
- Cloud Build
- Cloud CDN
- Cloud Composer
- Cloud Data Fusion
- Cloud Deployment Manager
- Cloud DNS
- Cloud Endpoints
- Cloud External Key Manager (Cloud EKM)
- Cloud Filestore
- Cloud Functions
- Cloud Functions for Firebase
- Cloud Healthcare
- Cloud HSM
- Cloud IDS (Cloud Intrusion Detection System)
- Cloud Interconnect
- Cloud Key Management Service
- Cloud Life Sciences
- Cloud Load Balancing
- Cloud Logging
- Cloud Monitoring
- Cloud NAT (Network Address Translation)
- Cloud Natural Language API
- Cloud NGFW
- Cloud Org Policy
- Cloud Profiler
- Cloud Router
- Cloud Run
- Cloud Scheduler
- Cloud Service Mesh
- Cloud Source Repositories
- Cloud Spanner
- Cloud Speaker ID
- Cloud SQL
- Cloud Storage
- Cloud Storage for Firebase
- Cloud Tasks
- Cloud Trace
- Cloud Translation
- Cloud Vision
- Cloud VPN

This scope is only valid in connection with certificate 2021-017.

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2021-017

Google Cloud Platform (continued):

- Cloud Workstations
- Compute Engine
- Connect
- Container Registry
- Conversational AI
- Conversational Insights
- Data Catalog
- Database Migration Service
- Dataflow
- Dataform
- Dataplex
- Dataproc
- Dataproc Metastore
- Datastore
- Datastream
- Dialogflow
- Document AI
- Document AI Warehouse
- Eventarc
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Gemini Code Assist
- Gemini for Google Cloud
- Gemini in BigQuery
- Generative AI on Vertex AI
- GKE Enterprise Config Management
- GKE Identity Service
- Google Cloud Armor
- Google Cloud Backup and DR
- Google Cloud Contact Center as a Service (CCaaS)
- Google Cloud Deploy
- Google Cloud Identity-Aware Proxy
- Google Earth Engine
- Google Kubernetes Engine
- Google Security Operations (SIEM)
- Google Security Operations (SOAR)
- GTI for Google Security Operations
- Healthcare Data Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- Integration Connectors
- Key Access Justifications (KAJ)
- Knative serving
- Looker (Google Cloud core)
- Looker Studio
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Migrate to Virtual Machines
- Migration Center
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- NotebookLM for enterprise
- Persistent Disk
- Pub/Sub
- reCAPTCHA Enterprise
- Recommendations AI
- Recommender
- Resource Manager API
- Retail Search
- Risk Manager
- Secret Manager
- Secure Source Manager
- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- Service Directory
- Service Infrastructure
- Service Mesh
- Spectrum Access System
- Speech-to-Text

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2021-017

Google Cloud Platform (continued):

- Storage Transfer Service
- Talent Solution
- Text-to-Speech
- Traffic Director
- Transcoder API
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Video Intelligence API
- Virtual Private Cloud
- VPC Service Controls
- Web Risk API
- Workflows
- Workload Manager

GCP Cloud Edge:

- Media CDN

Google Cloud NetApp Volumes (GCNV):

- Google Cloud NetApp Volumes

Google Cloud VMware Engine (GCVE):

- Google Cloud VMware Engine

The following locations are in scope:

Data Centers:

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Austin (TX), United States of America
- Berlin (1), Germany
- Berlin (2), Germany
- Berlin (3), Germany
- Chandler (AZ), United States of America
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Dalarna, Sweden
- Dammam, Saudi Arabia
- Dammam (2), Saudi Arabia
- Dammam (3), Saudi Arabia
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India
- Delhi (4), India
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2021-017

Data Centers (continued):

- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Frankfurt (9), Hesse, Germany
- Fredericia, Denmark
- Gainesville (VA), United States of America
- Ghlin, Hainaut, Belgium
- Guanajuato, Mexico
- Hamina, Finland
- Henderson (NV), United States of America
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia
- Johannesburg (1), South Africa
- Johannesburg (2), South Africa
- Johannesburg (3), South Africa
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Las Vegas (NV), United States of America
- Lancaster (OH), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Lok Yang Way, Singapore
- London (1), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Loyang, Singapore
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Markham, Ontario, Canada
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia
- Middenmeer, Noord-Holland, the Netherlands
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America
- Midlothian (3) (TX), United States of America
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada
- Montreal (2), Quebec, Canada
- Mumbai (1), India
- Mumbai (2), India
- Mumbai (3), India
- Mumbai (4), India
- Mumbai (5), India
- New Albany (OH), United States of America
- Omaha (NE), United States of America
- Osaka (1), Japan
- Osaka (2), Japan
- Osasco, Brazil

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2021-017

Data Centers (continued):

- Papillion (NE), United States of America
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Phoenix (AZ), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile
- Quilicura (3), Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- San Bernardo, Santiago, Chile
- Santana de Parnaíba, Brazil
- Seoul (1), South Korea
- Seoul (2), South Korea
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- The Dalles (3) (OR), United States of America
- Seoul (3), South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- The Dalles (2) (OR), United States of America
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Vinhedo, Brazil
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Wenya, Singapore
- Widows Creek (AL), United States of America
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland

Offices:

- Accra, Ghana
- Addison (TX), United States of America
- Amsterdam, the Netherlands
- Ann Arbor (MI), United States of America
- Athens, Greece
- Atlanta (GA), United States of America
- Auckland, New Zealand
- Austin (TX), United States of America
- Bangalore, India
- Bangkok, Thailand
- Barcelona, Spain
- Beijing, China
- Bellevue (WA), United States of America
- Belo Horizonte, Brazil
- Berlin, Germany
- Bogota, Colombia
- Boston (MA), United States of America

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2021-017

Offices (continued):

- Bothell (WA), United States of America
- Boulder (CO), United States of America
- Brisbane, Australia
- Brussels, Belgium
- Bucharest, Romania
- Budapest, Hungary
- Buenos Aires, Argentina
- Cairo, Egypt
- Calgary, Alberta, Canada
- Cambridge (MA), United States of America
- Cebu City, Philippines
- Charlotte (NC), United States of America
- Chicago (IL), United States of America
- Copenhagen, Denmark
- Detroit (MI), United States of America
- Doha, Qatar
- Dubai, United Arab Emirates
- Dublin, Ireland
- Durham (NC), United States of America
- Espoo, Finland
- Frankfurt, Germany
- Fremont (CA), United States of America
- Gandhinagar, India
- Gdansk, Poland
- Goleta (CA), United States of America
- Ghent, Belgium
- Gurgaon, India
- Haifa, Israel
- Hamburg, Germany
- Hanoi, Vietnam
- Helsinki, Finland
- Hong Kong, Hong Kong
- Houston (TX), United States of America
- Hyderabad, India
- Irvine (CA), United States of America
- Istanbul, Turkey
- Johannesburg, South Africa
- Kirkland (WA), United States of America
- Kitchener, Canada
- Krakow, Poland
- Kuala Lumpur, Malaysia
- Lagos, Nigeria
- Lima, Peru
- Lisbon, Portugal
- London, United Kingdom
- Los Angeles (CA), United States of America
- Madison (WI), United States of America
- Madrid, Spain
- Malaga, Spain
- Manchester, United Kingdom
- Manila, Philippines
- Melbourne, Australia
- Mexico City, Mexico
- Miami (FL), United States of America
- Milan, Italy
- Montreal, Québec, Canada
- Mountain View (CA), United States of America
- Mumbai, India
- Munich, Germany
- Nairobi, Kenya
- Nashville (TN), United States of America
- New Taipei City, Taiwan
- New York (NY), United States of America
- Osaka, Japan

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2021-017

Offices (continued):

- Oslo, Norway
- Ottawa, Ontario, Canada
- Palo Alto (CA), United States of America
- Paris, France
- Perth, Australia
- Pittsburgh (PA), United States of America
- Playa Vista (CA), United States of America
- Portland (OR), United States of America
- Poughkeepsie (NY), United States of America
- Prague, Czech Republic
- Princeton (NJ), United States of America
- Pune, India
- Quezon City, Philippines
- Ramat Gan, Israel
- Redmond (WA), United States of America
- Redwood City (CA), United States of America
- Reston (VA), United States of America
- Riyadh, Saudi Arabia
- Rome, Italy
- Salt Lake City (UT), United States of America
- San Bruno (CA), United States of America
- San Diego (CA), United States of America
- San Francisco (CA), United States of America
- San Jose (CA), United States of America
- Santa Cruz (CA), United States of America
- Santiago, Chile
- Sao Paulo, Brazil
- Seattle (WA), United States of America
- Seoul, South Korea
- Shanghai, China
- Shenzhen, China
- Singapore, Singapore
- South Jakarta, Indonesia
- South San Francisco (CA), United States of America
- Southaven (MS), United States of America
- Stockholm, Sweden
- Sunnyvale (CA), United States of America
- Sydney, Australia
- Taipei, Taiwan
- Taoyuan, Taiwan
- Tel Aviv, Israel
- Thornton (CO), United States of America
- Tokyo, Japan
- Toronto, Canada
- Vancouver, Canada
- Viby, Denmark
- Vienna, Austria
- Vilnius, Lithuania
- Virginia (VA), United States of America
- Warsaw, Poland
- Washington, D.C., United States of America
- Wroclaw, Poland
- Zagreb, Croatia
- Zhubei City, Taiwan
- Zurich, Switzerland

Docusign Envelope ID: AD9198E4-639F-4C64-B0B4-64AAFDEFA206

Google LLC

Scope for certificate 2021-017

The Privacy Information Management System (PIMS) is centrally managed out of the Google LLC headquarters in Mountain View, California, United States of America. The PIMS mentioned in the above scope is restricted as defined in 'Google Privacy Information Management System (PIMS) Implementation Manual', reviewed on May 23, 2025, by the Director and Global Head of Privacy for Google Cloud.

Google LLC (Google Cloud) provides consulting services to its customers. The consulting team "Google Cloud Professional Services Organization" is included in the Google Cloud PIMS.

Google Confidental Information



System and Organization Controls (SOC) 1 Type II Report
Description of the Google Cloud Platform System

For the Period 01 August 2024 to 31 July 2025

With Independent Service Auditor's Assurance Report

Including Tests Performed and Results Thereof

bernard@botmaker.io

Google Confidental Information

Table of Contents

SECTION I - Google's Management Assertion 1

SECTION II - Independent Service Auditor's Assurance Report 4

SECTION III - Description of the Google Cloud Platform System 9

A. Overview of Operations 10

B. Organization and Administration 44

C. Logical Access 47

D. Change Management 50

E. Physical Security 51

F. Incident Management 52

G. Availability 54

SECTION IV - Description of Control Objectives, Controls, Tests and Results of Tests 59

Testing performed and results of tests of entity level controls 60

Control objectives and related controls for systems and applications 60

CO1 - Organization and Administration 61

CO2 - Logical Access 79

CO3 - Change Management 98

CO4 - Physical Security 111

CO5 - Incident Management 120

CO6 - Availability 129

bernard@dotmaker.io

SECTION I - Google's Management Assertion

bernard@botmaker.io

Google Confidental Information

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Google's Management Assertion

We have prepared the description of Google's Google Cloud Platform System entitled, "Description of the Google Cloud Platform System" (Description) for the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) provided to user entities throughout the period 1 August 2024 to 31 July 2025 for user entities of the system during some or all of the period 1 August 2024 to 31 July 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Complementary user entity controls: The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Google's controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

(a) The Description fairly presents the Google Cloud Platform System (System) made available to user entities of the System during some or all of the period 1 August 2024 to 31 July 2025 for the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) provided to user entities as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

1. Presents how the System made available to user entities of the system was designed and implemented, including, if applicable:

    - The types of services provided
    - The procedures, within both automated and manual systems, by which those services are provided for user entities of the System
    - The information used in the performance of the procedures and supporting information; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities
    - How the System captures and addresses significant events and conditions
    - The process used to prepare reports and other information for user entities
    - Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them

bernard@bernard.pl

- The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls
- Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided

2. Includes relevant details of changes to the System during the period covered by the Description

3. Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors, and may not, therefore, include every aspect of the Google Cloud Platform System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment

(b) The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period 1 August 2024 to 31 July 2025 to achieve those control objectives, if user entities applied the complementary user entity controls assumed in the design of Google's controls throughout the period 1 August 2024 to 31 July 2025. The criteria we used in making this assertion were that:

1. The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization
2. The controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and
3. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority

bernd@bodmakers.ie

Google LLC
18 September 2025

SECTION II - Independent Service Auditor's Assurance Report

bernard@botmaker.io

Google Confidental Information

Shape the future with confidence

Ernst & Young LLP
303 Almaden Blvd
San Jose, CA 95110

Tel: +1 949 794 2300
Fax: +1 866 492 5140
ey.com

Independent Service Auditor's Assurance Report

To the Management of Google LLC:

Scope

We have examined Google LLC's (referred to hereafter as "Google") description entitled "Description of the Google Cloud Platform System" (Description) throughout the period 1 August 2024 to 31 July 2025 of its Google Cloud Platform system (System) for the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and provided to user entities and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in "Google's Management Assertion" (Assertion). The Control Objectives and controls included in the Description are those that management of Google believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

Complementary user entity controls: The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of Google's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Google's responsibilities

Google has provided the accompanying assertion titled, "Google's Management Assertion", about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. Google is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

bernard@counsel.com

Shape the future with confidence

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA") and International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period 1 August 2024 to 31 July 2025. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives, based on the criteria in management's Assertion
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved
- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion

Our examination was not conducted for the purpose of evaluating the performance or integrity of Google's AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Google's AI services.

We are required to be independent of Google and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA. We have complied with such independence and other ethical requirements and applied the AICPA's Statements on Quality Control Standards.

We apply International Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements*, which requires that we design, implement and operate a system of quality

Verrigbotmaker.it

Google Confidental Information

management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct all misstatements for the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) provided to user entities. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying "Section IV - Description of Control Objectives, Controls, Tests and Results of Tests" (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the criteria described in Google's Assertion:

(a) The Description fairly presents the System that was designed and implemented throughout the period 1 August 2024 to 31 July 2025
(b) The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period 1 August 2024 to 31 July 2025 and user entities applied the complementary controls assumed in the design of Google's controls throughout the period 1 August 2024 to 31 July 2025
(c) The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period 1 August 2024 to 31 July 2025 if the user entity controls assumed in the design of Google's controls operated effectively throughout the period 1 August 2024 to 31 July 2025

bernard@hotmail.fr

Google Confidental Information

Shape the future with confidence

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of Google, user entities of Google's System during some or all of the period 1 August 2024 to 31 July 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

18 September 2025
San Jose, CA

bernard@botmaker.io

SECTION III - Description of the Google Cloud Platform System

bernard@botmaker.io

Description of the Google Cloud Platform System

A. Overview of Operations

Google LLC (“Google” or “the Company”), an Alphabet subsidiary, is a global technology service provider focused on improving the ways people connect with information. Google’s innovations in web search and advertising have made Google’s website one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world’s largest online index of websites and other content, and makes this information freely available to anyone with an Internet connection. Google’s automated search technology helps people obtain nearly instant access to relevant information from their vast online index.

Google Cloud Platform provides Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS), allowing businesses and developers to build and run any or all of their applications on Google’s Cloud infrastructure. Customers can benefit from the performance, scale, reliability, ease-of-use, and a pay-as-you-go cost model.

Google’s product offerings for Google Cloud Platform (GCP) provide the unique advantage of leveraging the resources of Google’s core engineering team while also having a dedicated team to develop solutions for the corporate market. As a result, these Google offerings are positioned to innovate at a rapid rate and provide the same level of service that users are familiar with on google.com.

This report only applies to the underlying infrastructure and systems that support the services outlined below. The examination was also not conducted for the purpose of evaluating the performance or integrity of Google’s AI services or models.

Google Cloud Platform includes the following services, hereafter described collectively as “Google Cloud Platform” or "GCP":

- Artificial Intelligence (AI) and Machine Learning (ML) - Innovative, scalable machine learning services, with pre-trained models and the ability to generate tailored models
- Application Programming Interface (API) Management - Develop, deploy, and manage APIs on any Google Cloud back end
- Compute - A range of computing options tailored to match the size and needs of any organization
- Data Analytics - Tools to capture, process, store and analyze data on a single platform
- Databases - Migrate, manage, and modernize data with secure, reliable, and highly available relational and nonrelational databases
- Developer Tools - A collection of tools and libraries that help development teams work more quickly and effectively
- Healthcare and Life Sciences - Healthcare solution to protect sensitive data and maintain compliance with numerous requirements across various domains, geographies, and workloads

hernan@bonfake.io

- Hybrid and Multi-cloud - Connect on-premises or existing cloud infrastructure with Google Cloud's scalability and innovation
- Management Tools - Manage apps on GCP with a web-based console, mobile app, or Cloud Shell for real time monitoring, logging, diagnostics, and configuration
- Media and Gaming - Build user experiences and empower developers by minimizing infrastructure complexity and accelerating data insights
- Migration - Large-scale, secure online data transfers to Cloud Storage and databases
- Networking - A private network using software-defined networking and distributed systems technologies to host and deliver services around the world
- Operations - Suite of products to monitor, troubleshoot, and improve application performance on Google Cloud environments
- Security and Identity - Manage the security and access to cloud assets, supported by Google's own protection of its infrastructure
- Serverless Computing - Deploy functions or apps as source code or as containers without worrying about the underlying infrastructure. Build full stack serverless applications with Google Cloud's storage, databases, machine learning, and more
- Storage - Scalable storage options and varieties for different needs and price points
- Other - Additional GCP services supporting e-commerce, procurement, billing, and petabyte-scale scientific analysis and visualization of geospatial datasets

The Google Cloud Platform products covered in this system description consist of the following services:

- Artificial Intelligence (AI) and Machine Learning (ML)
- Agent Assist
- Agentspace[5]
- AI Platform Deep Learning Container
- AI Platform Training and Prediction[3]
- Anti-Money Laundering (AML) AI
- AutoML Tables
- AutoML Translation
- Cloud Natural Language API
- Cloud Speaker ID
- Cloud Translation
- Cloud Vision
- Conversational AI (formerly Contact Center AI (CCAI)
- Conversational Insights (formerly Contact Center AI Insights)
- Dialogflow
- Document AI
- Document AI Warehouse
- Food Ordering AI Agent
- Gemini Code Assist[5]

bernard@normaker.io

- Gemini for Google Cloud
- Gemini in BigQuery[5]
- Generative AI on Vertex AI
- Google Cloud Contact Center as a Service (CCaaS)
- NotebookLM for Enterprise[5]
- Ray on Vertex AI
- Recommendations AI
- Retail Search
- Speech-to-Text
- Talent Solution
- Text-to-Speech
- Vertex AI Codey[4]
- Vertex AI Colab Enterprise
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Vertex AI Workbench Instances
- Video Intelligence API

- Application Programming Interface (API) Management
  - Advanced API Security
  - Apigee
  - API Gateway
  - Application Integration
  - Cloud Endpoints
  - Integration Connectors
- Compute
  - App Engine
  - Batch
  - Compute Engine
  - Workload Manager
- Data Analytics
  - BigQuery
  - Cloud Composer
  - Cloud Data Fusion
  - Cloud Life Sciences
  - Data Catalog

bernard@hotmaker.io

Google Confidental Information

- Dataflow
- Dataform
- Dataplex
- Dataproc
- Dataproc Metastore
- Looker (Google Cloud core)
- Looker Studio
- Managed Service for Apache Kafka[1]
- Pub/Sub

- Databases
  - AlloyDB
  - Cloud Bigtable
  - Cloud Spanner
  - Cloud SQL
  - Datastore
  - Firestore
  - Memorystore

- Developer Tools
  - Artifact Analysis
  - Artifact Registry
  - Cloud Build
  - Cloud Source Repositories
  - Cloud Workstations
  - Container Registry
  - Firebase Test Lab
  - Google Cloud Deploy
  - Google Cloud SDK
  - Infrastructure Manager
  - Secure Source Manager

- Healthcare and Life Sciences
  - Cloud Healthcare
  - Healthcare Data Engine (HDE)

- Hybrid and Multi-cloud
  - Connect
  - Google Kubernetes Engine

bernard@botmaker.io

  - GKE Enterprise Config Management
  - GKE Identity Service
  - Hub
  - Knative serving
  - Service Mesh
- Management Tools
  - Cloud Console
  - Cloud Console App
  - Cloud Deployment Manager
  - Cloud Shell
  - Recommender
  - Service Infrastructure
- Media and Gaming
  - Media CDN
  - Transcoder API
- Migration
  - BigQuery Data Transfer Service
  - Database Migration Service
  - Migration Center
  - Migrate to Virtual Machines
  - Storage Transfer Service
- Networking
  - Cloud CDN
  - Cloud DNS
  - Cloud IDS (Cloud Intrusion Detection System)
  - Cloud Interconnect
  - Cloud Load Balancing
  - Cloud Network Address Translation (NAT)
  - Cloud NGFW
  - Cloud Router
  - Cloud Service Mesh
  - Cloud Virtual Private Network (VPN)
  - Google Cloud Armor
  - Network Connectivity Center
  - Network Intelligence Center

bernard@botmaker.io

Google Confidental Information

  - Network Service Tiers
  - Service Directory
  - Spectrum Access System
  - Traffic Director
  - Virtual Private Cloud (VPC)
- Operations
  - Cloud Logging
  - Cloud Monitoring
  - Cloud Profiler
  - Cloud Trace
  - Google Cloud Backup and DR
  - Personalized Service Health
- Security and Identity
  - Access Approval
  - Access Context Manager
  - Access Transparency
  - Assured Workloads
  - Binary Authorization
  - Certificate Authority Service
  - Certificate Manager
  - Chrome Enterprise Premium
  - Cloud Asset Inventory
  - Cloud External Key Manager (Cloud EKM)
  - Cloud Hardware Security Module (HSM)
  - Cloud Key Management Service (KMS)
  - Firebase App Check
  - Firebase Authentication
  - Google Cloud Identity-Aware Proxy
  - Google Threat Intelligence[2]
  - Google Security Operations (SIEM)[2]
  - Google Security Operations (SOAR)[2]
  - GTI for Google Security Operations[2]
  - Identity & Access Management (IAM)
  - Identity Platform
  - Key Access Justifications (KAJ)
  - Managed Service for Microsoft Active Directory (AD)
  - Organization Policy[1]

bernard@botmaker.io

- Privileged Access Manager
- reCAPTCHA Enterprise
- Resource Manager API
- Risk Manager
- SecLM
- Secret Manager
- Security Command Center
- Sensitive Data Protection (including Cloud Data Loss Prevention)
- VirusTotal
- VPC Service Controls
- Web Risk API

- Serverless Computing
  - Cloud Functions
  - Cloud Functions for Firebase
  - Cloud Run
  - Cloud Scheduler
  - Cloud Tasks
  - Datastream
  - Eventarc
  - Workflows

- Storage
  - Backup for GKE
  - Cloud Filestore
  - Cloud Storage
  - Cloud Storage for Firebase
  - Parallelstore[1]
  - Persistent Disk

- Other
  - Cloud Billing
  - Google Earth Engine
  - Google Cloud Marketplace
  - Google Cloud Skills Boost[1]
  - Tables

[1] Indicates products in scope only for the period 1 March 2025 through 31 July 2025

[2] Google Security Operations (SIEM), Google Security Operations (SOAR) and Google Threat Intelligence (GTI) for Google Security Operations are covered by separate terms than GCP. Refer

bernard@botmaker.io

to the Terms of Services (https://cloud.google.com/terms/secops/service-terms) for additional details

[3] The AI Platform Training & Prediction product was deprecated on January 31, 2025.

[4] The Vertex AI Codey product was deprecated on April 21, 2025.

[5] Indicates products only in scope for the period 1 May 2025 through 31 July 2025

The products are composed of communication, productivity, collaboration, and security tools that can be accessed from virtually any location with secure Internet connectivity. This means every employee and each user entity they work with can be productive from anywhere, using any device with a secure Internet connection.

These products provide a comprehensive variety of technical services that organizations rely on:

Artificial Intelligence (AI) and Machine Learning (ML)

Google does not use Customer Data to train or fine-tune any AI/ML models without a customer's prior permission or instruction. Refer to the service terms (https://cloud.google.com/terms/service-terms) for additional details.

Agent Assist

Agent Assist is a Large Language Model (LLM)- powered AI solution that increases human agent productivity and enhances customer service by offering real-time assistance.

Agentspace

Agentspace combines AI Agents, Gemini models, and Google search technologies to enable automation and enhance employee productivity by connecting enterprise data sources and applications, offering workflow automation, search functionality, and generative AI features.

AI Platform Deep Learning Container

AI Platform Deep Learning Container provides Docker images with AI frameworks that can be customized and used with Google Kubernetes Engine (GKE), Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.

AI Platform Training and Prediction

AI Platform Training and Prediction is a managed service that enables users to easily build machine learning models with popular frameworks like TensorFlow, XGBoost and Scikit Learn. It provides scalable training and prediction services that work on large datasets.

Anti-Money Laundering (AML) AI

AML AI is a machine learning engine which takes customer data and training labels to create a tailored model covering an extensible typology of risks for AML along with governance documentation to ease adoption in this highly regulated environment.

bernard@hotmaker.io

AutoML Tables

AutoML Tables enables data scientists, analysts, and developers to automatically build and deploy machine learning models on structured data at increased speed and scale.

AutoML Translation

AutoML Translation is a simple and scalable translation solution that allows businesses and developers with limited machine learning expertise to customize the Google Neural Machine Translation (GNMT) model for their own domain or use-case.

Cloud Natural Language API

Cloud Natural Language API provides natural language understanding as a simple to use Application Programming Interface (API). Given a block of text, this API enables finding entities, analyzing sentiment (positive or negative), analyzing syntax (including parts of speech and dependency trees), and categorizing the content into a rich taxonomy. The API can be called by passing the content directly or by referring to a document in Cloud Storage.

Cloud Speaker ID

Speaker ID allows customers to enroll user voice prints and later verify users against a previously enrolled voice print.

Cloud Translation

Cloud Translation automatically translates text from one language to another language (e.g., French to English). The API is used to programmatically translate text in webpages or apps.

Cloud Vision

Cloud Vision enables the understanding of image content by encapsulating machine learning models in a Representational State Transfer (REST) API. It classifies images into thousands of categories, detects individual objects and faces within images, and finds and reads printed words contained within images. It can be applied to build metadata on image catalogs, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. It can also analyze images uploaded in the request and integrate with image storage on Google Cloud Storage.

Conversational AI (formerly Contact Center AI (CCAI)

Conversational AI uses AI to improve the customer experience in contact centers. It includes Agent Assist, Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Insights, Speech-to-Text, Text-to-Speech, and Speaker ID.

Conversational Insights (formerly Contact Center AI Insights)

Conversational Insights helps customers extract value from their contact center data by identifying sentiment and topics and highlighting key insights in the data.

bernard@botmaker.io

Google Confidental Information

Dialogflow

Dialogflow is a development suite for voice and text conversational apps including chatbots. Dialogflow is cross-platform and can connect to apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Actions on Google, Facebook Messenger, Slack).

Document AI

Document AI classifies and extracts structured data from documents to help streamline data validation and automate business processes.

Document AI Warehouse

Document AI Warehouse is a data management and governance platform that stores, searches, and organizes documents and their extracted and tagged metadata. Document AI Warehouse is highly scalable and fully managed and can be integrated with enterprise document workflows, applications, and repositories.

Food Ordering AI Agent

A repeatable, scalable Food Ordering Voice Assistant that helps restaurants serve their customers with high quality and consistent service.

Google Cloud Contact Center as a Service (CCaaS)

Google Cloud CCaaS is a contact-center-as-a-service (CCaaS) platform leveraging Conversational AI. It integrates directly with CRMs and queues and routes customer interactions across voice and digital channels to resource pools, including human agents.

Gemini Code Assist

Gemini Code Assist provides AI-powered assistance to help customer development teams build, deploy, and operate applications throughout the software development lifecycle.

Gemini for Google Cloud

Gemini for Google Cloud provides AI-powered end user assistance with a wide range of Google Cloud products. Gemini for Google Cloud is a generative AI-powered collaboration Service that provides assistance to Google Cloud end users. Gemini for Google Cloud is embedded in many Google Cloud products to provide developers, data scientists, and operators an integrated assistance experience.

Gemini in BigQuery

Gemini in BigQuery provides AI-powered assistance to help customers understand, query, and work with their data across the entire data lifecycle.

Generative AI on Vertex AI

Generative AI on Vertex AI includes features for generative AI use cases, including large language, text-to-image, and image-to-text models.

bernard@hotmaker.it

NotebookLM for Enterprise

NotebookLM for enterprise enables customers to use generative AI to summarize and extract information from their data.

Ray on Vertex AI

Ray on Vertex AI is an open-source framework for scaling AI and Python applications. Ray provides the infrastructure to perform distributed computing and parallel processing for the user's machine learning (ML) workflow.

Recommendations AI

Recommendations AI enables customers to build a personalized recommendation system using ML models.

Retail Search

Retail Search allows retailers to leverage Google's search capabilities on their retail websites and applications.

Speech-to-Text

Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy-to-use API.

Talent Solution

Talent Solution offers access to Google's machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.

Text-to-Speech

Text-to-Speech synthesizes human-like speech based on input text in a variety of voices and languages.

Vertex AI Codey

Vertex AI Codey is a suite of models that work with code that includes the following APIs:

- The code generation API - Generates code based on a natural language description of the desired code.
- The code chat API - Can power a chatbot that assists with code-related questions.
- The code completion API - Provides code autocompletion suggestions as users write code.

Vertex AI Colab Enterprise

Vertex AI Colab Enterprise is a collaborative, managed notebook environment with the security and compliance capabilities of Google Cloud.

bernard@botmaker.io

Vertex AI Conversation

Vertex AI Conversation allows customers to leverage foundational models and conversational AI to create multimodal chat or voice agents.

Vertex AI Platform

Vertex AI Platform is a service for managing the AI and machine learning development lifecycle. Customers can (i) store and manage datasets, labels, features, and models; (ii) build pipelines to train and evaluate models and run experiments using Google Cloud algorithms or custom training code; (iii) deploy models for online or batch use cases; (iv) manage data science workflows using Colab Enterprise and Vertex AI Workbench (also known as Notebooks); and (v) create business optimization plans with Vertex Decision Optimization.

Vertex AI Search

Vertex AI Search allows customers to leverage foundational models and search and recommendation technologies to create multimodal semantic search and question-answering experiences.

Vertex AI Workbench Instances

Vertex AI Workbench instances are Jupyter notebook-based development environments for the entire data science workflow. Users can interact with Vertex AI and other Google Cloud services from within a Vertex AI Workbench instance's Jupyter notebook.

Video Intelligence API

Video Intelligence API makes videos searchable, and discoverable, by extracting metadata through a REST API. It annotates videos stored in Google Cloud Storage and helps identify key noun entities in a video and when they occur within the video.

API Management

Advanced API Security

Advanced API Security acts as the users' API's vigilant guardian. It constantly analyzes incoming traffic, seeking out anomalous patterns that might indicate attacks or abuse. When suspicious activity is spotted, it can block harmful requests or alert users for further action. Additionally, it evaluates the users' API setups against security best practices, offering recommendations for improvement. This comprehensive approach helps users proactively safeguard the users' APIs, protect sensitive data, and ensure the users' API configurations are designed to withstand security challenges.

Apigee

Apigee is a full-lifecycle API management platform that lets customers design, secure, analyze, and scale APIs, giving them visibility and control. Apigee is available as Apigee, a fully managed service, Apigee hybrid, a hybrid model that's partially hosted and managed by the customer, or

bernard@netmaker.io

Apigee Private Cloud, an entirely customer hosted Premium Software solution. Apigee Private Cloud is not in scope for this report.

API Gateway

API Gateway is a fully managed service that enables users to develop, deploy, and secure APIs running on Google Cloud Platform.

Application Integration

Application Integration is an Integration-Platform-as-a-Service (iPaaS) that offers a comprehensive set of integration tools to connect and manage the multitude of applications and data required to support various business operations. Application Integration provides a unified drag and drop integration designer interface, triggers that help invoke an integration, configurable tasks and numerous connectors that allow connectivity to business applications, technologies, and other data sources using the native protocols of each target application.

Cloud Endpoints

Cloud Endpoints is a tool that provides services to develop, deploy, secure and monitor APIs running on Google Cloud Platform.

Integration Connectors

Integration Connectors is a platform that allows customers to connect to business applications, technologies and other data sources using native protocols of each target application. The connectivity established through these connectors helps manage access to various data sources which can be used with other services like Application Integration through a consistent, standard interface.

Compute

App Engine

App Engine enables the building and hosting of web apps on the same systems that power Google applications. App Engine offers fast development and deployment of applications without the need to manage servers or other low-level infrastructure components. Scaling and software patching are handled by App Engine on the user's behalf. App Engine also provides the ability to create managed virtual machines (VMs). In addition, client APIs can be built for App Engine applications using Google Cloud Endpoints.

Batch

Batch is a fully managed service that lets users schedule, queue, and execute batch processing workloads on Compute Engine virtual machine (VM) instances. Batch provisions resources and manages capacity on users’ behalf, allowing user batch workloads to run at scale.

Compute Engine

Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud. With virtual machines that can boot in minutes, it offers many configurations including custom

bernardo@otmaker.io

Google Confidental Information

machine types that can be optimized for specific use cases as well as support for Graphics Processing Units (GPUs), Tensor Processing Units (TPUs) and Local Solid-State Drive (SSD). Additionally, customers can enable Shielded VMs to provide advanced platform security.

Workload Manager

Workload Manager is a rule-based validation service for evaluating workloads running on Google Cloud. If enabled, Workload Manager scans application workloads to detect deviations from standards, rules, and best practices that improve system quality, reliability, and performance.

Data Analytics

BigQuery

BigQuery is a fully managed, petabyte-scale analytics data warehouse that features scalable data storage and the ability to perform ad hoc queries on multi-terabyte datasets. BigQuery allows users to share data insights via the web and control access to data based on business needs.

Cloud Composer

Cloud Composer is a managed workflow orchestration service that can be used to author, schedule, and monitor pipelines that span across clouds and on-premises data centers.

Cloud Data Fusion

Cloud Data Fusion is a fully managed, cloud native, enterprise data integration service for building and managing data pipelines. Cloud Data Fusion provides a graphical interface that allows customers to build scalable data integration solutions to cleanse, prepare, blend, transfer, and transform data.

Cloud Life Sciences

Cloud Life Sciences is a suite of services and tools to store, process, inspect and share biomedical data, DNA sequence reads, reference-based alignments, and variant calls, using Google's cloud infrastructure.

Data Catalog

Data Catalog is a fully managed and scalable metadata management service that allows organizations to have a centralized and unified view of data assets.

Dataflow

Dataflow is a fully managed service for consistent, parallel data-processing pipelines. It utilizes the Apache Beam Software Development Kits (SDKs) with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the lifecycle of Compute Engine resources for the processing pipeline(s) and provides a monitoring interface for understanding pipeline health.

bernard@hotmaker.it

Dataform

Dataform is a service for data analysts to develop, test, version control, and schedule complex SQL workflows for data transformation in BigQuery. Dataform lets users manage data transformation in the Extraction, Loading, and Transformation (ELT) process for data integration. After raw data is extracted from source systems and loaded into BigQuery, Dataform helps users to transform it into a well-defined, tested, and documented suite of data tables.

Dataplex

Dataplex is an intelligent data fabric that helps customers unify distributed data and automate management and governance across that data to power analytics at scale.

Dataproc

Dataproc is a managed service for distributed data processing. It provides management, integration, and development tools for deploying and using Apache Hadoop, Apache Spark, and other related open source data processing tools. With Cloud Dataproc, clusters can be created and deleted on-demand and sized to fit whatever workload is at hand.

Dataproc Metastore

Dataproc Metastore provides a fully-managed metastore service that simplifies technical metadata management and is based on a fully-featured Apache Hive metastore. Dataproc Metastore can be used as a metadata storage service component for data lakes built on open source processing frameworks like Apache Hadoop, Apache Spark, Apache Hive, Presto, and others.

Looker (Google Cloud core)

Looker (Google Cloud core) is a business intelligence and embedded analytics solution hosted on Google infrastructure. With Looker (Google Cloud core), customers can build semantic models using various data sources, develop customized insights from the models, and share those insights for collaboration via dashboards and other services.

Looker Studio

Looker Studio is a visualization and business intelligence product that enables users to connect to multiple datasets and turn their data into informative, easy to share, and fully customizable dashboards and reports.

Managed Service for Apache Kafka

Managed Service for Apache Kafka is a Google Cloud service that helps you run secure, scalable open source Apache Kafka clusters.

Pub/Sub

Pub/Sub provides reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a topic while other applications can subscribe to

bernard@netmaker.io

that topic to receive the messages. By decoupling senders and receivers, Cloud Pub/Sub allows communication between independent applications.

Databases

AlloyDB

AlloyDB is an enterprise grade database product that combines the familiarity of open source DB front-ends, like PostgreSQL, with custom-built storage, query and connectivity layers for superior availability, performance, security and manageability.

Cloud Bigtable

Cloud Bigtable is a low-latency, fully managed, highly scalable NoSQL database service. It is designed for the retention and serving of data from gigabytes to petabytes in size.

Cloud Spanner

Cloud Spanner is a fully managed, scalable, relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and ACID (Atomicity, Consistency, Isolation, Durability) transactions with synchronous replication of data across regions.

Cloud SQL

Cloud SQL is a service to create, configure, and use managed third-party relational databases in Google Cloud Platform. Cloud SQL maintains, manages, and administers those databases.

Datastore

Datastore is a highly scalable NoSQL database for mobile and web applications. It provides query capabilities, atomic transitions, index, and automatically scales up and down in response to load.

Firestore

Firestore is a fully managed, scalable, serverless NoSQL document database for mobile, web, and server development. It provides query capabilities, live synchronization, and offline support.

Memorystore

Memorystore for Redis (Remote Dictionary Server) provides a fully managed in-memory data store service for GCP. Cloud Memorystore can be used to build application caches that provide low latency data access. Cloud Memorystore is compatible with the Redis protocol, allowing seamless migration with no code changes.

Developer Tools

Artifact Analysis

Artifact Analysis is a family of services that provide software composition analysis, metadata storage and retrieval. Its detection points are built into a number of Google Cloud products such as Artifact Registry and Google Kubernetes Engine (GKE) for quick enablement. The service

bernard@hotmail.io

works with both Google Cloud's first-party products and also lets users store information from third-party sources. The scanning services leverage a common vulnerability store for matching files against known vulnerabilities.

Artifact Registry

Artifact Registry is a service for managing container images and packages. It is integrated with Google Cloud tooling and runtimes and comes with support for native artifact protocols. This makes it simple to integrate it with user CI/CD tooling to set up automated pipelines.

Cloud Build

Cloud Build allows for the creation of container images from application source code located in Cloud Storage or in a third-party service (e.g., Github, Bitbucket). Created container images can be stored in Container Registry and deployed on Container Engine, Compute Engine, App Engine Flexible Environment, or other services to run applications from Docker containers.

Cloud Source Repositories

Cloud Source Repositories provides Git version control to support collaborative development of any application or service as well as a source browser that can be used to browse the contents of repositories and view individual files from within the Cloud Console. Cloud Source Repositories and related tools (e.g., Cloud Debugger) can be used to view debugging information alongside code during application runtime.

Cloud Workstations

Cloud Workstations provides preconfigured, customizable, and secure managed development environments on Google Cloud. Cloud Workstations is accessible through a browser-based Integrated Development Environment (IDE), from multiple local code editors (such as IntelliJ IDEA Ultimate or VS Code), or through SSH. Instead of manually setting up development environments, users can create a workstation configuration specifying user environments in a reproducible way.

Container Registry

Container Registry is a private Docker image storage system on Google Cloud Platform.

Firebase Test Lab

Firebase Test Lab provides cloud-based infrastructure for testing apps on physical and virtual devices. Developers can test their apps across a wide variety of devices with Firebase Test Lab.

Google Cloud Deploy

Google Cloud Deploy is a managed service that automates delivery of user applications to a series of target environments in a defined promotion sequence. When users want to deploy updated applications, users create a release, whose lifecycle is managed by a delivery pipeline.

bernard@bonfaker.io

Google Cloud SDK

Google Cloud SDK is a set of tools to manage resources and applications hosted on Google Cloud Platform. It includes the Google Cloud Command Line Interface (CLI), Cloud Client Libraries for programmatic access to Google Cloud Platform services, the gsutil, kubectl, and bq command line tools, and various service and data emulators for local platform development. The Google Cloud SDK provides the primary programmatic interfaces to Google Cloud Platform.

Infrastructure Manager

Infrastructure Manager is a managed service that automates the deployment and management of Google Cloud infrastructure resources. Infrastructure is defined using Terraform and deployed onto Google Cloud by Infra Manager, enabling users to manage resources using Infrastructure as Code (IaC).

Secure Source Manager

Secure Source Manager is a fully-managed service that provides a Git-based source code management system.

Healthcare and Life Sciences

Cloud Healthcare

Cloud Healthcare provides managed services and an API to store, process, manage, and retrieve healthcare data in a variety of industry standard formats.

Healthcare Data Engine (HDE)

HDE is a solution that enables (1) harmonization of healthcare data to the Fast Healthcare Interoperability Resources (“FHIR”) standard and (2) streaming of healthcare data to an analytic environment.

Hybrid and Multi-cloud

The scope of the services included in this report is limited to the services managed by Google and does not extend to the application of the services in other cloud service providers' environments by the user entity. Refer to the Terms of Services (https://cloud.google.com/terms/services) for additional details.

Connect

Connect is a service that allows users to connect Kubernetes clusters to Cloud. This enables both users and Google-hosted components to interact with clusters through a connection to the in-cluster Connect software agent.

Google Kubernetes Engine

Google Kubernetes Engine, powered by the open source container scheduler Kubernetes, runs containers on Google Cloud Platform. Kubernetes Engine manages provisioning and maintaining

bernard@botmaker.io

the underlying virtual machine cluster, scaling applications, and operational logistics such as logging, monitoring, and cluster health management.

GKE Enterprise Config Management

GKE Enterprise Config Management is a policy management solution for enabling consistent configuration across multiple Kubernetes clusters. GKE Enterprise Config Management allows customers to specify one single source of truth and then enforce those policies on the clusters.

GKE Identity Service

GKE Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple environments. Users can log in to and access their clusters from the command line or from the Cloud Console, all using their existing identity providers.

Hub

Hub is a centralized control-plane that enables a user to centrally manage features and services on customer-registered clusters running in a variety of environments, including Google's cloud, on-premises in customer data centers, or other third-party clouds.

Knative serving

Knative serving is Google's managed and fully supported Knative offering. Knative serving abstracts away the complexity of Kubernetes, making it easy to build and deploy user's serverless workloads across hybrid and multi-cloud environments.

Service Mesh

Service Mesh is a managed service mesh service that includes (i) a managed certificate authority that issues cryptographic certificates that identify customer workloads within the Service Mesh for mutual authentication, and (ii) telemetry for customers to manage and monitor their services. Customers receive details showing an inventory of services, can understand their service dependencies, and receive metrics for monitoring their services. Service Mesh is provided as a service and as a software. The Service Mesh software offering is not in scope for this report.

Management Tools

Cloud Console

Cloud Console is a web-based interface used to build, modify, and manage services and resources on the Google Cloud Platform. Cloud services can be procured, configured, and run from Cloud Console.

Cloud Console App

Cloud Console App is a native mobile app that provides monitoring, alerting, and the ability to take actions on resources.

leonard@lootmaker.io

Google Confidental Information

Cloud Deployment Manager

Cloud Deployment Manager is an infrastructure management service which automates creation, and management of Google Cloud Platform resources.

Cloud Shell

Cloud Shell provides command-line access to Google Cloud Platform resources through an in-browser Linux shell backed by a temporary Linux VM in the cloud. It allows projects and resources to be managed without having to install additional tools on systems and comes equipped and configured with common developer tools such as text editors, a MySQL client and Kubernetes.

Recommender

Recommender automatically analyzes usage patterns to provide recommendations and insights across services to help use Google Cloud Platform in a more secure, cost-effective, and efficient manner.

Service Infrastructure

Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services. It includes:

- Service Management API, which lets service producers manage their APIs and services;
- Service Consumer Management API, which lets service producers manage their relationships with their service consumers;
- Service Control API, which lets managed services integrate with Service Infrastructure for admission control and telemetry reporting functionality; and
- Service Usage API, which lets service consumers manage their usage of APIs and services

Media and Gaming

Media CDN

Media CDN is a planet-scale content delivery network allowing customers to automate all facets of deployment and management. Stream media and deliver exceptional experiences to customer end users, no matter where they are.

Transcoder API

Transcoder API can batch convert media files into optimized formats to enable streaming across web, mobile, and living room devices. It provides fast, easy to use, large-scale processing of advanced codecs while utilizing Google's storage, networking, and delivery infrastructure.

Migration

BigQuery Data Transfer Service

BigQuery Data Transfer Service automates data movement from Software as a Service (SaaS) applications to BigQuery on a scheduled, managed basis.

bernal@hotmaker.io

Database Migration Service

Database Migration Service is a fully managed migration service that enables users to perform high fidelity, minimal-downtime migrations at scale. Users can use Database Migration Service to migrate from on-premises environments, Compute Engine, and other clouds to certain Google Cloud-managed databases.

Migration Center

Migration Center provides tools, best practices and data-driven prescriptive guidance designed to accelerate the end-to-end cloud migration journey through business case development, environment discovery, workload mapping, migration planning, financial analysis, foundation setup and migration execution.

Migrate to Virtual Machines

Migrate to Virtual Machines is a fully-managed migration service that enables customers to migrate workloads at scale into Google Cloud Compute Engine with minimal down time by utilizing replication-based migration technology.

Storage Transfer Service

Storage Transfer Service provides the ability to import large amounts of online data into Google Cloud Storage. It can transfer data from Amazon Simple Storage Service (Amazon S3) and other HTTP/HTTPS locations as well as transfer data between Google Cloud Storage buckets.

Networking

Cloud CDN

Cloud Content Delivery Network (CDN) uses Google's distributed network edge points of presence to cache HTTP(S) load balanced content.

Cloud DNS

Cloud DNS is a fully managed Domain Name System (DNS) service which operates a geographically diverse network of high-availability authoritative name servers. Cloud DNS provides a service to publish and manage DNS records for applications and services.

Cloud IDS (Cloud Intrusion Detection System)

Cloud IDS is a managed service that aids in detecting certain malware, spyware, command-and-control attacks, and other network-based threats.

Cloud Interconnect

Cloud Interconnect offers enterprise-grade connections to Google Cloud Platform. This solution provides direct connection between on-premise networks and GCP Virtual Private Cloud.

bernard@hotmaker.io

Cloud Load Balancing

Cloud Load Balancing is a distributed, software-defined, managed service for all traffic (HTTP(S), TCP/SSL, and UDP) to computing resources. Cloud Load Balancing rapidly responds to changes in traffic, network, backend health and other related conditions.

Cloud Network Address Translation (NAT)

Cloud Network Address Translation (NAT) enables virtual machine instances in a private network to communicate with the Internet, without external IP addresses.

Cloud NGFW

Cloud NGFW is a fully distributed, cloud-native firewall service that evaluates incoming and outgoing traffic on a network, according to user-defined firewall rules in the policy.

Cloud Router

Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between a Virtual Private Cloud (VPC) network and an external network, typically an on-premise network.

Cloud Service Mesh

Cloud Service Mesh is a service mesh available on Google Cloud and across supported GKE Enterprise platforms. It supports services running on a range of computing infrastructures. Cloud Service Mesh is controlled by APIs designed for Google Cloud, for open source, or for both.

Cloud Virtual Private Network (VPN)

Cloud Virtual Private Network (VPN) provides connections between on-premises or other external networks to Virtual Private Clouds on GCP via an IPsec connection or can be used to connect two different Google managed VPN gateways.

Google Cloud Armor

Google Cloud Armor provides access control configurations and at-scale defenses to help protect infrastructure and applications against distributed denial-of-service (DDoS), application-aware and multi-vector attacks.

Network Connectivity Center

Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud that facilitates connecting a customer's resources to its cloud network.

Network Intelligence Center

Network Intelligence Center provides a single console for managing Google Cloud's comprehensive network monitoring, verification, and optimization platform across the Google Cloud, multi-cloud, and on-premises environments.

bernard@hotmail.it

Network Service Tiers

Network Service Tiers enable the selection of different quality networks (tiers) for outbound traffic to the Internet: Standard Tier primarily utilizes third-party transit providers while Premium Tier leverages Google's private backbone and peering surface for egress.

Service Directory

Service Directory is a managed service that offers customers a single place to publish, discover and connect their services in a consistent way, regardless of their environment. Service Directory supports services in Google Cloud, multi-cloud and on-premises environments and can scale up to thousands of services and endpoints for a single project.

Spectrum Access System

Spectrum Access System enables users to access the Citizens Broadband Radio Service (CBRS) in the United States, the 3.5 GHz band that is available for shared commercial use. Users can use Spectrum Access System to register CBRS devices, manage CBRS deployments, and access a non-production test environment.

Traffic Director

Traffic Director is Google Cloud Platform's traffic management service for open-source service meshes.

Virtual Private Cloud (VPC)

Virtual Private Cloud is a comprehensive set of managed networking capabilities for Google Cloud resources including granular IP address range selection, routes and firewalls.

Operations

Cloud Logging

Cloud Logging is a hosted solution that helps users gain insight into the health, performance and availability of their applications running on Google Cloud Platform and other public cloud platforms. It includes monitor dashboards to display key metrics, define alerts and report on the health of cloud systems. The components of Cloud Logging that run on other public cloud platforms are not in scope for this report.

Cloud Monitoring

Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from certain Services, hosted uptime probes, application instrumentation, alert management, notifications and a variety of application components.

Cloud Profiler

Cloud Profiler continuously gathers and reports source-level performance information from production services. It provides key information to determine what functions in code consume the

bernard@bolmaker.io

most memory and CPU cycles so insights can be gained on how code operates to improve performance and optimize computing resources.

Cloud Trace

Cloud Trace collects latency data from applications and displays it in the Google Cloud Platform Console. It automatically analyzes trace data to generate in-depth performance reports that help identify and locate performance bottlenecks.

Google Cloud Backup and DR

Google Cloud Backup and DR is a managed backup and disaster recovery service for centralized protection of workloads in Google Cloud.

Personalized Service Health

Personalized Service Health, which lets users identify Google Cloud service disruptions relevant to user's projects so users can manage and respond to them efficiently. These disruptions are called service health events, and are available in the Google Cloud console and a variety of integration points.

Security and Identity

Access Approval

Access Approval allows customers to approve eligible manual, targeted access by Google administrators to their data or workloads prior to access being granted.

Access Context Manager

Access Context Manager allows customer administrators to define attribute-based access control for projects, apps and resources.

Access Transparency

Access Transparency captures near real-time logs of certain manual, targeted accesses by Google personnel, and provides them via Cloud Logging accounts.

Assured Workloads

Assured Workloads provides functionality to create security controls that are enforced on customer cloud environment and can assist with compliance requirements (e.g. FedRAMP Moderate compliance).

Binary Authorization

Binary Authorization helps customers ensure that only signed and explicitly authorized container images are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.

bernard@hotmaker.io

Certificate Authority Service

Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Customers can use Certificate Authority Service to create certificate authorities using Cloud KMS keys to issue, revoke, and renew subordinate and end-entity certificates.

Certificate Manager

Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the certificates.

Chrome Enterprise Premium

Chrome Enterprise Premium is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware and phishing attacks. Chrome Enterprise Premium is an integrated platform incorporating cloud-based services and software components.

Cloud Asset Inventory

Cloud Asset Inventory is a service that allows customers to view, monitor, and analyze cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.

Cloud External Key Manager (Cloud EKM)

Cloud EKM lets customers encrypt data in Google Cloud Platform with encryption keys that are stored and managed in a third-party key management system deployed outside Google's infrastructure.

Cloud Hardware Security Module (HSM)

Cloud HSM is a cloud-hosted Hardware Security Module (HSM) service for hosting encryption keys and performing cryptographic operations.

Cloud Key Management Service (KMS)

Cloud KMS is a cloud-hosted key management service that manages encryption for cloud services. It enables the generation, use, rotation, and destruction of encryption keys.

Firebase App Check

Firebase App Check provides a service that can help protect access to user’s APIs with platform specific attestation that helps verify app identity and device integrity.

Firebase Authentication

Firebase Authentication is a fully managed user identity and authentication system providing backend services enabling sign-in and sign-up experiences for an application or service.

bernard@bitmaker.io

Google Cloud Identity-Aware Proxy

Google Cloud Identity-Aware Proxy (Cloud IAP) is a tool that helps control access to applications running on Google Cloud Platform based on identity and group membership.

Google Threat Intelligence

Google Threat Intelligence combines the unmatched depth of our Mandiant frontline expertise, the global reach of the VirusTotal community, and the breadth of visibility only Google can deliver, based on billions of signals across devices and emails. Google Threat Intelligence includes Gemini in Threat Intelligence, our AI-powered agent that provides conversational search across our vast repository of threat intelligence, enabling customers to gain insights and protect themselves from threats faster than ever before. The Attack Surface Management (ASM) and Digital Threat Monitoring (DTM) features of Google Threat Intelligence are Mandiant products and maintain equivalent certifications.

Google Security Operations (SIEM)

Google Security Operations Security Information and Event Management (SIEM) enables enterprise security teams to detect, investigate, and respond to threats at speed and scale. Chronicle SIEM does this by collecting security telemetry data, aggregating it, normalizing it, and applying threat intelligence to identify the highest priority threats.

Google Security Operations (SOAR)

Google Security Operations Security Orchestration, Automation and Response (SOAR) is a platform designed to help organizations detect, investigate, and respond to security threats in real-time. The platform is powered by Google Cloud's infrastructure and leverages the machine learning capabilities of Google to automate and streamline security workflows.

GTI for Google Security Operations

GTI for Google Security Operations is a service extension for Google Security Operations (SIEM) that hunts for threats in external customer environments. This effort includes active research for new and emerging threats. It also includes focused batch hunting that extracts suspicious logs warranting either special review or logs that should be automatically sent to customers

Identity & Access Management (IAM)

Identity & Access Management (IAM) enables the administration and authorization of accesses to specific resources and provides a unified view into security policies across entire organizations with built-in auditing.

Identity Platform

Identity Platform is a customer identity and access management (CIAM) platform delivered by Google Cloud enabling organizations to add identity management and user security to their applications or services.

jernano@bonmaker.io

Key Access Justifications (KAJ)

Key Access Justifications (KAJ) provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at-rest to in-use.

Managed Service for Microsoft Active Directory (AD)

Managed Service for Microsoft Active Directory (AD) is a Google Cloud service running Microsoft AD that enables customers to deploy, configure and manage cloud-based AD-dependent workloads and applications. It is a fully managed service that is highly available, applies network firewall rules, and keeps AD servers updated with Operating System patches.

Privileged Access Manager

Privileged Access Manager (PAM) allows customers to control just-in-time temporary privilege elevation for select principals, and to view audit logs afterwards to find out who had access to what and when.

Organization Policy

Organization Policy provides customizable security guardrails to centrally enforce resource configuration compliance across resource hierarchies.

reCAPTCHA Enterprise

reCAPTCHA Enterprise helps detect fraudulent activity on websites using risk analysis techniques to distinguish between humans and bots.

Resource Manager API

Resource Manager API allows users to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects) to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization enables users to manage common aspects of resources such as access control and configuration settings.

Risk Manager

Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including CIS benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.

SecLM

SecLM or more specifically, the SecLM Platform (formerly known as Security AI Workbench or SAW) - refers to the API and platform that is built based on the SecPaLM models. The platform orchestrates reasoning, extensions, retrieval augmented generation (RAG), and other techniques to leverage authoritative security data from sources, like Mandiant Advantage Threat Intelligence (MATI) and VirusTotal, and deliver the highest quality responses to security-related prompts.

bernard@hotmaker.it

Google Confidental Information

Secret Manager

Secret Manager provides a secure method for storing API keys, passwords, certificates, and other sensitive data.

Security Command Center

Security Command Center is a log monitoring and security scanning tool that generates analytics and dashboards to help customers to prevent, detect, and respond to Google Cloud security and data threats.

Sensitive Data Protection (including Cloud Data Loss Prevention)

Sensitive Data Protection is a fully-managed service enabling customers to discover, classify, de-identify, and protect sensitive data, such as personally identifiable information.

VirusTotal

VirusTotal enables organizations to research and hunt for malware, to investigate security incidents, to automate analysis, and to keep user investigations private and secure.

VPC Service Controls

VPC Service Controls provides administrators with the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks.

Web Risk API

Web Risk API is a Google Cloud service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.

Serverless Computing

Cloud Functions

Cloud Functions is a serverless compute solution that runs single-purpose functions in response to GCP events and HTTP calls (webhooks). Cloud Functions can be triggered asynchronously by Cloud Pub/Sub, Cloud Storage, GCP infrastructure events, and Firebase products. Cloud Functions scales automatically to meet request load and the user does not need to manage servers or the runtime environment.

Cloud Functions for Firebase

Cloud Functions for Firebase are developer tools used for development and deployment of Google Cloud Functions. Cloud Functions enable developers to run their own backend code that executes automatically based on HTTP requests and Firebase and Google Cloud Platform events. Developers' functions are stored in Google’s cloud and run in a managed Node.js environment.

bernard@bormaker.io

Google Confidental Information

Cloud Run

Cloud Run (fully managed) is a serverless, managed compute platform that automatically scales stateless HTTP containers, running requests or event-driven stateless workloads. Cloud Run provides the flexibility to run services on a fully managed environment.

Cloud Scheduler

Cloud Scheduler is a fully managed enterprise-grade cron job scheduler. It allows customers to schedule jobs, including batch, big data jobs, cloud infrastructure operations, and more. It also acts as a single interface for managing automation tasks, including retries in case of failure to reduce manual toil and intervention.

Cloud Tasks

Cloud Tasks is a fully managed service that allows customers to manage the execution, dispatch, and delivery of a large number of distributed tasks.

Datastream

Datastream is a serverless and easy-to-use change data capture (CDC) and replication service that allows users to synchronize data streams across heterogeneous databases and applications reliably and with minimal latency. Datastream supports streaming changes to data from Oracle and MySQL databases into Cloud Storage.

Eventarc

Eventarc is a fully managed service for eventing on Google Cloud Platform. Eventarc connects various Google Cloud services together, allowing source services (e.g., Cloud Storage) to emit events that are delivered to target services (e.g., Cloud Run or Cloud Functions).

Workflows

Workflows is a fully managed service for reliably executing sequences of operations across microservices, Google Cloud services, and HTTP-based APIs.

Storage

Backup for GKE

Backup for GKE enables data protection for workloads running in Google Kubernetes Engine clusters.

Cloud Filestore

Cloud Filestore is a service for fully managed Network File System (NFS) file servers for use with applications running on Compute Engine virtual machines (VMs) instances or Google Kubernetes Engine clusters.

bernard@botmaker.io

Google Confidental Information

Cloud Storage

Cloud Storage is Google Cloud Platform's unified object/blob storage. It is a RESTful service for storing and accessing data on Google Cloud Platform's infrastructure. It combines the simplicity of a consistent API and latency across different storage classes with reliability, scalability, performance and security of Google Cloud Platform.

Cloud Storage for Firebase

Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for Firebase apps. Cloud Storage for Firebase is backed by Cloud Storage, a service for storing and accessing data on Google's infrastructure.

Parallelstore

Parallelstore is a parallel file system for high-performance computing and AI/ML workloads. Built on the Distributed Asynchronous Object Storage (DAOS) architecture, Parallelstore combines a fully distributed metadata and key-value architecture to deliver high-performance throughput and IOPS.

Persistent Disk

Persistent Disk provides a persistent virtual disk for use with Google Compute Engine and Google Kubernetes Engine compute instances. It is available in both SSD (Solid State Drive) and HDD (Hard Disk Drive) variations.

Other

Cloud Billing

Cloud Billing provides methods to programmatically manage billing for projects on the Google Cloud Platform.

Google Earth Engine

Google Earth Engine combines a multi-petabyte catalog of satellite imagery and geospatial datasets with planetary-scale analysis capabilities. Scientists, researchers, and developers can use Earth Engine to detect changes, map trends, and quantify differences on the Earth's surface.

Google Cloud Marketplace

Google Cloud Marketplace offers ready-to-go development stacks, solutions, and services from third-party partners and Google to accelerate development. It enables the deployment of production-grade solutions, obtains direct access to partner support, and receives a single bill for both GCP and third-party services.

Google Cloud Skills Boost

Google Cloud Skills Boost is where you can access Google Cloud’s entire catalog of labs and courses. Customer end users can discover learning paths, build in-demand cloud skills, track your activity progress, and validate your knowledge with badges.

bernard@botmakers.io

Tables

Tables is a lightweight collaborative database to help organize and automate tasks or processes for small teams and businesses.

Data Centers

The above products are serviced from data centers operated by Google around the world. Below is a list of Google's production data center locations that host the above products and operations for Google Cloud Platform. The scope of this report does not cover Google edge points of presence (PoPs).

North America, South America

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Austin (TX), United States of America**
- Chandler (AZ), United States of America
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Gainesville (VA), United States of America
- Guanajuato, Mexico
- Henderson (NV), United States of America
- Lancaster (OH), United States of America
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Markham, Ontario, Canada
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America*
- Midlothian (3) (TX), United States of America***
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada

bernard@hotmaker.io

- Montreal (2), Quebec, Canada
- New Albany (OH), United States of America
- Omaha (NE), United States of America
- Osasco, Brazil
- Papillion (NE), United States of America
- Phoenix (AZ), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile
- Quilicura (3), Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America
- San Bernardo, Santiago, Chile
- Santana de Parnaíba, Brazil
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- The Dalles (3) (OR), United States of America**
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada
- Vinhedo, Brazil
- Widows Creek (AL), United States of America

Europe, Middle East, and Africa

- Berlin (1), Germany
- Berlin (2), Germany
- Berlin (3), Germany
- Dammam, Saudi Arabia
- Dammam (2), Saudi Arabia*
- Dammam (3), Saudi Arabia*
- Dalarna, Sweden
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, The Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany

bernard@botmaker.io

- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Frankfurt (9), Hesse, Germany**
- Fredericia, Denmark
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- Johannesburg (1), South Africa
- Johannesburg (2), South Africa
- Johannesburg (3), South Africa
- London (1), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Middenmeer, Noord-Holland, The Netherlands
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland

bernard@botmaker.io

Google Confidental Information

Asia Pacific

- Changhua, Taiwan
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India
- Delhi (4), India***
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Lok Yang Way, Singapore
- Loyang, Singapore
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia
- Mumbai (1), India
- Mumbai (2), India
- Mumbai (3), India
- Mumbai (4), India
- Mumbai (5), India***
- Osaka (1), Japan
- Osaka (2), Japan
- Seoul (1), South Korea
- Seoul (2), South Korea
- Seoul (3), South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Wenya, Singapore

* Indicates data center is in scope only for the period 1 November 2024 through 31 July 2025

** Indicates data center is in scope only for the period 1 March 2025 through 31 July 2025

bernard@botmaker.io

*** Indicates data center is in scope only for the period 1 May 2025 through 31 July 2025

B. Organization and Administration

Control Objective 1

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Internal Control Environment

Google has designed its internal control environment with the objective of providing reasonable assurance as to the integrity and availability of the data and user information, as well as the protection of assets from unauthorized use or disposition. Management has established and maintains an internal control structure that monitors compliance with established policies and procedures.

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform products or services to customers. The fundamentals underlying the services provided are the adoption of standardized, repeatable processes, the hiring and development of highly skilled resources, and leading industry practices.

Formal organizational structures exist and are available to Google personnel, including employees, temporary workers, vendors, and contractors on the Company's intranet. The intranet provides drill-down functionality for identifying personnel in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Security and privacy policies are reviewed annually, and other materials derived from policies, like guidelines, frequently asked questions (FAQs), and other related documents are reviewed and updated as needed. Databases and web sites exist to track and monitor the progress of Google Cloud Platform project developments. Google establishes agreements, including non-disclosure agreements, for preserving the confidentiality of information and software exchange with external parties.

To maintain internal compliance, Google has established a disciplinary process for non-compliance with the Code of Conduct, company policies, and other personnel requirements which could include dismissal, lawsuits and/or criminal prosecution. Moreover, Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product related controls over change management, access management, configuration management, security management, redundancy management, incident management, and capacity management.

The organization utilizes technologies to support the workforce in both remote and office work environments.

internal@bohmayer.no

Information and Communication

To help align its business strategies and goals with operating performance and controls, Google has implemented various methods of communication to help ensure that all interested parties and personnel understand their roles and responsibilities and to help ensure that significant events are communicated in a timely manner. These methods include:

- Orientation and training programs for newly hired employees
- An information security training program that is required to be completed by relevant personnel annually
- Organization personnel are required to acknowledge the code of conduct
- Regular management meetings for updates on business performance and other business matters
- Company goals and responsibilities are developed and communicated by management on a periodic basis and amended as needed. Results are evaluated and communicated to employees
- Detailed job descriptions, product information (including system and its boundaries), and Google's security, availability, and confidentiality obligations that are made available to employees in the intranet
- The use of electronic mail messages to communicate time-sensitive messages and information
- Publishing security policies and security related updates in the intranet, which is accessible by all Google employees, temporary workers, contractors, and vendors

Google has also implemented various methods of communication to help ensure that user entities understand Google's commitments to security, availability, and confidentiality for Google Cloud Platform; and to help ensure that significant events are communicated to user entities in a timely manner. The primary conduit for communication is the Google website, which is made available to all user entities. This includes blog postings on the Official Google Blog, various product specific blogs, support forums and release notes. Google provides 24 x 7 assistance, including online and phone support to address customers' concerns. Customer service and/or technical support representatives are also an important communication channel, as they maintain records of problems reported by the user entity. Customer service representatives also assist in communicating information regarding new issues and/or developments, changes in services, and other information. Additionally, Google maintains an established Board of Directors that operates independently from management. The Board exercises oversight over management decisions.

Information Security Program

Google's Information Security program is designed to safeguard information assets against unauthorized use, disclosure, modification, damage, or loss. The program includes educating Google personnel about security related issues, assessing current policies and developing new policies, assisting in strengthening technical measures to protect corporate resources, and

kenard@botmaker.ro

developing mechanisms to react to incidents and events that could affect Google's information assets.

Google has dedicated security teams responsible for educating Google personnel about security and assisting product teams with security design. Information security is managed by a dedicated Security and Privacy executive who is independent of Information Technology management responsibilities and may escalate security issues or concerns directly to the board. The Security Team also reviews the security practices of vendors and the security posture of vendor products for all vendors that Google shares confidential or sensitive information with.

Google has security policies that have been reviewed and approved by management and are published and communicated to employees and extended workforce (i.e. temporary workers, vendors, and contractors) with access to the Google intranet. Google's security policies describe security objectives, provide a security framework, and emphasize the importance of security to Google's business. Security policies are reviewed at least annually. Policies, FAQs, and guidelines are updated as needed.

Hiring Practices

Google has designed formal global hiring practices to help ensure that new, rehired, or transferred employees are qualified for their functional responsibility. Every employee has a written job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Google. Where local labor law or statutory regulations permit, Google may conduct criminal, credit, and/or security checks on all potential employees, temporary workers, and independent contractors, as well as verification of the individual's education, previous employment, and referrals. The specifics or extent of background checks performed depend on the position and location for which the individual is applying.

Upon acceptance of employment, all employees including extended workforce personnel are required to execute a confidentiality agreement as well as acknowledge receipt and compliance with Google's Code of Conduct. The confidentiality and privacy of customer data is emphasized in the handbook and also during new employee orientation. It is the responsibility of every employee to timely communicate significant issues and exceptions to an appropriate higher level of authority within the Company.

Risk Management

Risk management is a pervasive component of Google Cloud Platform's products, irrespective of the location or business area. The Google teams which lead engineering, sales, customer service, finance, and operations have the primary responsibility to understand and manage the risks associated with their activities for user entities using Google Cloud Platform's products. These risk management and mitigation activities have been integrated into Google's repeatable process model.

At a corporate level there are multiple functional areas including: Legal, Information Security, Internal Audit, Global Directive Assurance (performing first party audit), Privacy Engineering, Compliance Assurance and Advisory, CSRM (Compliance, Security, and Risk Management),

bernard@bunmaker.no

Ethics and Business Integrity, RCI (Risk, Compliance and Integrity), Regulatory Affairs, and PSS (Privacy, Security and Safety), that provide risk management support through policy guidelines and internal consulting services.

Google develops and maintains a risk management framework to manage risk to an acceptable level for the Google Cloud Platform. Google has developed vulnerability management guidelines and regularly analyzes the vulnerabilities associated with the system environment. Google takes into consideration various threat sources such as insider attacks, external attacks, errors and omissions, and threats related to third parties such as the inadvertent disclosure of Google confidential information (for example, payroll data) by a third party.

Monitoring

Management performs periodic assessments of the control environment including areas such as identity management, source code management, physical security, and authentication infrastructure controls. Google's internal compliance team also performs regular internal audits and independent third-party audits over these areas of the control environment. The reports associated with these internal audits are reviewed in executive meetings and made available to the audit committee and stakeholders. In addition, monitoring activities have been described below to communicate how monitoring is performed for the Google Cloud Platform.

Data Retention and Deletion

Google maintains defined terms regarding the return, transfer, and disposal of user data and makes these terms available to customers.

C. Logical Access

Control Objective 2

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Network Architecture and Management

The Google Cloud Platform system architecture utilizes a fully redundant network infrastructure. Border routers that provide the connection point between Google Cloud Platform and any Internet Service Providers are designed to run in a redundant configuration. Where border routers are in use, firewalls are also implemented to operate in a redundant configuration.

Google has implemented perimeter devices to protect the Google network from external network attacks and configurations of perimeter devices are centrally managed. Google segregates networks based on the types of services, users, and information systems. Network monitoring mechanisms are in place to detect and prevent access to the Google network from unauthorized devices. The network is managed via specialized tools. Google employs automated tools to inventory network devices and machines. Authorized security and network engineers access the network devices (production routers and switches) to monitor, maintain, manage, and secure the network through these tools.

bernard@notmaker.io

Authentication, Authorization, and Administration

Authentication and access controls are implemented to restrict access to Google Cloud Platform production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) and Secure Sockets Layer (SSL) certificates, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google uses encryption to secure user data in transit between Google production facilities.

Access to internal support tools, those used by Google operational staff to maintain and troubleshoot the systems for Google Cloud Platform is controlled via access control lists (ACLs) thus limiting the use of these tools to only those individuals that have been authorized. Digital certificates used for machine authentication and data encryption are issued by an internal Google certificate authority. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to the Google corporate machines requires a Google-issued digital certificate installed on the connecting device and two-factor authentication.

Google follows a formal process to grant or revoke personnel access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system, which utilizes Secure Shell (SSH) and TLS/SSL certificates, help provide secure and flexible access. These mechanisms are designed to grant access rights to systems and data only to authorized users. Additionally, access requests via "on demand" mechanisms are reviewed and approved by an authorized second individual prior to being granted and the event is logged.

Both user entities and internal access to customer data are restricted by using unique user account IDs and via the Google Accounts Bring Your Own Identity (BYOID) system for external users. Access to sensitive systems and applications requires two-factor authentication in the form of unique user IDs, strong passwords, and security keys; and/or a certificate. Periodic reviews of access lists are implemented to help ensure access to customer data (and other need-to-know data) is appropriate and authorized. Access to production machines, network devices, and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semiannual basis under the direction of the group administrators, and any inappropriate access identified is removed.

Access authorization in Google Cloud Platform is enforced at all relevant layers of the system. The granting or modification of access rights is based on the user's job responsibilities or on a need-to-know basis and must be authorized and approved by the user's functional manager or system owners. Approvals are managed by workflow tools and are logged. Production system access is only granted to individuals who require this level of access to perform necessary tasks. Additionally, all users with access to production systems are required to complete security and privacy training annually. Access to individual production systems via critical access groups is reviewed on a periodic basis by the system owners and inappropriate access is removed for Google personnel who no longer have a business need for such access. Access to all corporate and production resources is automatically removed upon submission of a termination request by

vernal@moonkey.io

the manager of any departing employee, temporary worker, contractor or vendor, or by the appropriate Human Resources manager.

Password Guidelines

Google personnel are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following:

- Minimum length
- Complexity
- History
- Idle time lockout setting

Password configuration requirements are enforced by internal systems. In addition to the security requirements enforced during configuration, internal passwords are subject to cryptographic hashing to mitigate the risk of unauthorized disclosure or modification.

Google has supplemented passwords with a two-factor authentication requirement for internal personnel to access sensitive internal corporate and production services and to access Google Cloud Platform in the production environment from the corporate network. Two-factor authentication provides additional protection to prevent user account manipulation in case the user's password is compromised.

Google Cloud Platform end-users can also authenticate in one of three ways:

- Using their user ID and a password that is managed by Google
- Using a two-step authentication process that includes their user ID, password, and a security key
- Through the Security Assertion Markup Language (SAML) based Single Sign-On (SSO) process which uses the user entity's own account management system to authenticate users and a certificate with an embedded public key, which is registered with Google for each customer entity.

Security Monitoring

Google has implemented monitoring tools to detect and report security events. Antivirus, phishing detection, secure coding, and antimalware/antispam tools are in place to protect Google's information assets. Google also maintains and protects security event logs for privileged access, access to user data, authorized, and unauthorized access attempts. Security event logs are monitored continuously using a Google proprietary Security Information and Event Management (SIEM) system to detect intrusion attempts and other security related events. The SIEM is supplemented with codified logic which creates the "hunts" that trigger automated alerts to security personnel. The security alerts are triaged through manual or automated actions and further investigated based on predefined thresholds.

bernard@bonnaki.jp

D. Change Management

Control Objective 3

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Overview

Changes to Google Cloud Platform are delivered as software releases through three (3) pipelines:

- Product functionality changes or builds related to the service running in Google's production environment;
- Images, downloads, or software updates made available to customers; and
- Open source code packages maintained in a public source code repository.

Changes including configuration changes, code modifications, and new code creation, follow this change management process. Change Management policies and guidelines, including code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented. Each service has documented release processes that specify the procedures to be used, including definition of the scope of changes to be delivered, source code control, code review, building, testing, and record keeping. Development, testing, and build environments are separated from the production environment through the use of logical security controls.

The change process starts with a developer checking out a copy of source code files from the source code management system to modify them. Once development is complete, the developer initiates applicable testing and code reviews. Once the change has received the appropriate code review, the change can be submitted making it the new head version. Google requires that production code reviewers be independent of the developer assigned to the change and follows Google coding standards, in accordance with their policy. Production code reviews are systematically enforced. Emergency changes to production environments must have a valid justification, and are logged, monitored and reviewed.

If needed, once the code is submitted, it can be used to build packages or binaries. During the build process, code is subject to automated testing, the results of which are monitored by engineers. Successfully built packages or binaries can be migrated to staging or QA environments where they can be subject to additional review. When the approved change is ready for deployment to production, it is deployed in a controlled manner, with monitoring in place to notify engineers of anomalies in the deployment. The process from build to release is aided by several tools that automate tasks, including testing and deployment. Employees at Google have the ability to view changes, however, access to modify code and approve changes is controlled via functionality of internal tools that support the build and release process. Changes to customer facing services that may affect confidentiality, processing integrity, and/or availability are communicated to relevant personnel and impacted customers. Please note, implementations and customizations by end-user customers after source code has been made available by Google in the public repositories are out of scope.

ljmd@bormaker.io

Guidelines are made available internally to govern the installation of software on organization-owned assets. Additionally, tools are utilized to automatically synchronize operating system (OS) configurations on production machines and correct them if deviations from the baseline image are detected. This enables a consistent deployment of updates to system files and helps ensure that machines remain in a known current-state. Mobile code is also blocked by default via standard web browser configurations on company owned endpoints.

E. Physical Security

Control Objective 4

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Overview

Google maintains consistent policies and standards across its data centers for physical security to help protect production servers, network devices, and network connections within Google Data Centers. Guidelines for evaluating the security of data centers are described in Google's Data Center security evaluation criteria. Additionally, data center personnel perform periodic surveys and reviews of data centers. Data centers that house Google Cloud Platform systems and infrastructure components are reviewed and assessed periodically for ongoing security compliance. A security report is then created summarizing any observations, deviations, or action items. This report is presented to executive management for review and approval. Corrective actions are taken when necessary. The data center security evaluation criteria elements include:

- Existence of security guards, access badges, and video cameras
- Entrances, cages, suites, and rooms in use by Google are secured by either badge readers, secondary identification mechanisms, and/or physical locks
- Emergency exit points from server rooms are alarmed
- Video cameras exist to monitor the interior and exterior of the facility
- 24 x 7 on-site security personnel

Formal access procedures exist for allowing physical access to the data centers. There are documented procedures for issuing badges to staff and/or visitors and the owner of each badge is tracked and documented. All entrants to the data center, whether they are Google employees, visitors, or contractors, must identify themselves as well as show proof of identity to Security Operations.

Valid proof of identity consists of a photo ID issued by (1) Google or (2) a governmental entity. Only validated visitors and authorized Google employees and contractors are permitted to enter the data centers. Authorized Google Data Center Approvers must approve all visitors in advance for the specific data center and internal areas they wish to visit.

After the individual's access authorization is verified, the visit is logged, and access is granted for the specified dates and times. These logs are retained by Google security for review as needed.

bernard@bonfaker.io

Visitors are provided a temporary badge and must be escorted by an authorized Google employee. When the visitors leave the data center, they must return the visitor badge.

Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas. Google authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items. Google also utilizes automated mechanisms to track inventory of all production machines and inventory of all serialized server components. Only authorized Google employees or contractors permanently working at the data centers are permitted to request standing access to the facility areas needed for their role and responsibilities. Data center access requests must be made through internal tools and require the approval of authorized data center personnel. All other Google employees and authorized contractors requiring temporary data center access must also have an approved access request and register at the guard station upon arrival. User access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.

Data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network infrastructure are connected to redundant power sources that are physically protected from disruption and damage in addition to emergency power which is available in the event of a loss of power. Google performs preventative and regular maintenance on fire detection and protection equipment, Uninterruptible Power Supply (UPS), generators, HVAC, and emergency lighting systems. Refer to Section A for a list of Google's Data Center locations.

bernard@bonnaker.io

F. Incident Management

Control Objective 5

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Incident Management

Dedicated on-call personnel and incident response teams are responsible for managing, responding to, and tracking incidents. These teams are organized into formalized shifts and are responsible for helping resolve emergencies 24 x 7. Incident response policies are in place and procedures for handling incidents are documented.

Incident Alert and Recording

Automated signals generate alerts whenever an anomaly occurs. Production monitoring tools, in response to an anomaly, automatically generate alerts to relevant teams. An anomaly may also be manually documented by Google personnel when an issue is identified in response to a customer service request or reported through externally available channels.

Production systems are configured to send system events to monitoring and alerting tools. Google personnel use these tools to respond to potential incidents, including, but not limited to, security incidents.

Alerts capture information necessary for initial response (e.g., origin, service description, impacted area, etc.). Alerts are addressed by relevant teams to identify if the anomaly indicates an issue or potential issue. If necessary, incidents are created for alerts that require additional investigation. Additional details can be added to the incident to supplement the initial alert(s). The incident is assigned an initial severity level, which is used to prioritize mitigation efforts to incidents of greatest severity. Each severity level has been formally defined to capture the importance of each incident/problem type. There are established roles and responsibilities for personnel tasked with incident management, including the identification, assignment, managed remediation, and communication of incidents.

Incident Escalation

Google has documented escalation procedures and communication protocols that address the handling of incidents and notifying appropriate individuals. Escalated issues are treated with higher urgency and often shared with a wider audience.

Alert escalation is facilitated by an internal escalation tool or manual escalation based on Google-wide and team-specific escalation criteria. Production monitoring tools are integrated with the alert manager tool and communicated with the escalation tool. The escalation time and contacts are defined in the escalation tool configuration files. This leads to automated escalation if the tool does not receive an acknowledgement from the notified contacts.

Incident Resolution

After gathering the necessary information about the incident, the incident ticket is assigned to the appropriate support area based on the nature of the problem and/or the root cause. Incidents are usually forwarded to one of the corresponding technical departments:

- System Reliability Engineers / Software Engineers
- Networks
- Database Administration
- System Administration
- Application Administration
- Facilities
- Network Security
- Platform Support

The incident ticket is closed upon resolution of the incident. Google also has an established process for performing technical analysis of incidents after the fact to identify root cause issues, document lessons learned, and implement fixes to strengthen and improve security controls, and to prevent future incidents.

permanente@bonnaker.ro

Google Confidental Information

G. Availability

Control Objective 6

Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.

Overview

Google Cloud Platform runs in a multi-tenant, distributed environment on synchronized internal system atomic clocks and global positioning systems (GPS). Rather than segregating user-entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For Google Cloud Platform, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Customer data is then stored in large, distributed databases, built on top of this file system. Where applicable, alternate storage procedures are documented and in place for backing up and recovering customer data. Backups are periodically performed to support the availability of customer data, and restore tests are periodically performed to confirm the ability to recover user data.

Redundant architecture exists such that data is replicated in real-time to at least two geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Management of the data centers is also distributed to provide location-independent, around the clock coverage and system administration. Google uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location. Additionally, business continuity plans defining how personnel should respond to disruptions are made available internally and maintained.

bernd@lotriker.io

H. Complementary User Entity Control Considerations

Google Cloud Platform is designed with the assumption that user entities (also referred to as customers) would implement certain policies, procedures, and controls. In certain situations, the application of specific or additional controls at the user entity may be necessary to achieve the control objectives stated in the description. Therefore, each user's controls must be evaluated in conjunction with the controls summarized in Section III and Section IV of this report.

This section describes those additional policies, procedures, and controls that Google recommends user entities should consider to complement Google's policies, procedures, and controls. Management of the user entity and the user entity's auditor should consider whether the following controls have been placed in operation at the user entity:

Google Confidental Information

Control Objective	Complementary User Entity Controls (CUECs)
CO1 - Organization and Administration: Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Cloud Platform System. Customers are also responsible for reviewing the information security policies and the security capabilities in the Google Cloud Platform System to determine their applicability and modify their internal controls as appropriate.
	Customers are responsible for providing the appropriate training to end-users on proper use of the Google Cloud Platform System consistent with the Acceptable Use Policies and Terms of Service, as well as any other organizational policies and procedures relevant to the use of the Google Cloud Platform System. Acceptable Use Policies available at (or such URL as Google may provide): • Google Cloud Platform: https://cloud.google.com/terms/aup • Chronicle (Security Product) and Threat Intelligence for Chronicle: https://chronicle.security/legal/service-terms/ https://chronicle.security/legal/acceptable-use-policy/
	Customers are responsible for defining, documenting, and making available to users procedures for the operation of their instance of the Google Cloud Platform System.
	Customers are responsible for identifying and managing the inventory of information assets on the Google Cloud Platform System.
	Customers are responsible for establishing organizational policies and procedures for the use or integration of third-party services, including documented policies and procedures for the transfer and sharing of information within their organization and with third-party entities.
CO2 - Logical Access: Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.	Customers are responsible for assigning responsibilities for the operation and monitoring of the Google Cloud Platform System.
	Customers are responsible for defining and maintaining policies and procedures governing the customer's administration of access to the Google Cloud Platform System.
	Customers are responsible for provisioning service availability, user roles, and sharing permissions within the Google Cloud Platform System consistent with customer organizational policies.

bernadette.mario@

Control Objective	Complementary User Entity Controls (CUECs)
	Customers are responsible for implementing secure log- on procedures to access the Google Cloud Platform System, and provisioning, maintaining, and disabling users' access consistent with customer access management policies.
	Customers are responsible for reviewing users' access rights periodically, consistent with customer organizational policies, to mitigate the risk of inappropriate access.
	Customers are responsible for establishing procedures to allocate the initial password to access the Google Cloud Platform System to end-users when Google password authentication is used, and for enabling and enforcing the use of two-step verification on privileged administrator accounts.
	Customers are responsible for training users on the use and disclosure of passwords used to authenticate to the Google Cloud Platform System.
	Customers are responsible for configuring GCP Marketplace permissions in Google Cloud Platform consistent with customer's internal policies (GCP Marketplace contains enterprise applications that can be added to a Google Cloud Platform).
	Customers are responsible for restricting access to and monitoring the use of Application Programming Interfaces (APIs) available in the Google Cloud Platform System.
	Customers are responsible for configuring domain settings related to integration with other systems within the customer's environment and for configuring the Google Cloud Platform System mobile device options consistent with customer policies and procedures.
	Customers are responsible for the deployment, configuration and modification of default security settings for cloud products including virtual machines in accordance with their information security requirements.
	Customers are responsible for providing permission or instructions to utilize their data and defining the scope of data for training or fine-tuning AI/ML models.
CO3 - Change Management: Controls provide reasonable assurance that changes to applications and	Customers are responsible for ensuring any application software which they deploy onto the Google Cloud Platform System follows their specific software change management policies and procedures. The customer is responsible for

bernadette@bmaeric.com

Control Objective	Complementary User Entity Controls (CUECs)
infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.	implementing any custom code necessary for the deployment of the products, and any code from public repositories for customization of their implementations.
	Customers are responsible for the training, testing, and deploying of AI models that are used in AI-powered applications.
	Customers are responsible for periodically reviewing the configuration of the Google Cloud Platform System to help ensure it is consistent with their policies and procedures.
	Customers are responsible for ensuring that user data is exported and deleted from the Google Cloud Platform System before or within a reasonable amount of time after termination.
	Customers are responsible for ensuring that individuals creating and/or updating profiles or changing the product configurations are authorized.
	Customers are responsible for reviewing and testing features, builds, and product releases, including Application Programming Interfaces (APIs), to evaluate their impact prior to deploying into production environments, as applicable.
	Customers are responsible for configuring test and/or development environments in their instance of the Google Cloud Platform System, as applicable, and restricting access to data in these environments.
	Customers are responsible for managing and testing configurations that support their business and operational resiliency objectives, and for considering Google Cloud Platform architecture recommendations.
CO4 - Physical Security: Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.	Customers are responsible for ensuring appropriate physical security controls over all devices that access the Google Cloud Platform System.
	Customers are responsible for ensuring any devices that access the Google Cloud Platform System or contain customer data are properly handled, secured, and transported as defined by the product's requirements.

bernardo@otmkeio

Google Confidental Information

Control Objective	Complementary User Entity Controls (CUECs)
CO5 - Incident Management: Controls provide reasonable assurance that application and system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.	Customers should establish and train administrators and end-users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of the Google Cloud Platform System.
	Customers should contact Google if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account, compromise of data, and security events.
CO6 - Availability: Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.	Customers are responsible for ensuring they have business recovery and backup procedures over their non-Google managed information systems that access the Google Cloud Platform System.
	Customers are responsible for configuring data storage locations that support their business and operational resiliency requirements.

bernard@botmaker.io

Google Confidental Information

SECTION IV - Description of Control Objectives, Controls, Tests and Results of Tests

bernard@botmaker.io

Google Confidental Information

Description of Control Objectives, Controls, Tests and Results of Tests

Testing performed and results of tests of entity level controls

In planning the nature, timing and extent of our testing of the controls specified by Google LLC, we considered the aspects of Google's control environment, risk assessment process, communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Sample sizes were selected using based on the nature of the control (e.g., automated or manual), the frequency of the control, and the available population.

Google centrally manages the majority of the controls from their headquarters in Mountain View, CA. However, certain physical security controls are operated at the individual data centers as listed in the system description. To help ensure controls are consistently designed and implemented across the data centers, the data center security team performs a review of each data center annually that is reviewed and approved by Google management. We perform site visits of the data centers on a rotation schedule to corroborate, through independent procedures (including observation and inspection), the controls are implemented as described within Google's review. We designed the visit schedule to ensure that each data center is visited at least once every three years and that new in-scope data centers are visited in the period they are brought into scope. Additionally, we inquired of management regarding any known control deviations identified during management's internal testing. Where any material deviations were noted, we have included the results in the procedures performed.

Control objectives and related controls for systems and applications

On the pages that follow, the applicable control objectives and the controls to achieve the objectives have been specified by, and are the responsibility of, Google LLC. The sections "Tests Performed by EY" and "Results" are the responsibility of Ernst & Young LLP.

For tests of controls requiring the use of Information Produced by the Entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), EY performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the IPE, (2) inspected the query, script, or parameters used to generate the IPE, (3) tied data between the IPE and the source, and/or (4) inspected the IPE for anomalous gaps in sequence or timing to determine the data was complete, accurate, and maintained its integrity. Furthermore, in addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings); we inspect management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

bernard@boomerang.io

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
1. The organization has policies and guidelines that govern the acceptable use of information assets.	Inquired of the Program Manager and determined the organization established policies and procedures that governed the acceptable use of information assets.	No deviations noted.
	Inspected the relevant documentation and determined Google established policies and procedures that governed the acceptable use of information assets.	No deviations noted.
2. The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	Inquired of the Program Manager and determined the organization established a disciplinary process to address non-compliance with company policies, code of conduct, or other personnel requirements.	No deviations noted.
	Inspected internal documentation and determined the organization established a disciplinary process for non-compliance with the company policies, code of conduct, or other personnel requirements which could result in dismissal, lawsuits and/or criminal prosecution.	No deviations noted.
	Inspected the disciplinary procedures undertaken for sample incidents and determined appropriate action was taken in cases of non-compliance with company policies, code of conduct, or other personnel requirements.	No deviations noted.
3. The organization has established a code of conduct that is reviewed and updated as needed.	Inquired of the Program Manager and determined the organization established a code of conduct that was reviewed and updated as needed.	No deviations noted.
	Inspected applicable policies and guidelines and determined the privacy and information security procedures as well as the code of conduct were in place and reviewed and updated as needed.	No deviations noted.

bernd.v@boilmaker.io

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
4. The organization has implemented a formal reporting structure that is made available to personnel.	Inquired of the Program Manager and determined the organization implemented a formal reporting structure that was made available to personnel.	No deviations noted.
	Inspected the organization's intranet and determined organizational charts showing formal reporting structure were made accessible to employees and included drill-down functionality to identify employees within the organizational structure, including employees in their functional teams.	No deviations noted.
	Inspected a sample communication and determined top level management changes were communicated internally and externally.	No deviations noted.
	Inspected the meeting minutes of a sample Board of Directors forum and determined management considered requirements such as integrity and security when defining authorities, structures, reporting lines, and responsibilities.	No deviations noted.
	Inspected procedural documents and determined management planned and prepared for succession by developing contingency plans for assignments of responsibility.	No deviations noted.
5. The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inquired of the Program Manager and determined the organization had a vulnerability management program in place to detect and remediate system vulnerabilities.	No deviations noted.
	Inspected internal policies and guidelines and determined the organization had a vulnerability management program in place to identify, detect, report, prioritize, and remediate system vulnerabilities.	No deviations noted.

bernard@baumer.ie

Google Confidental Information

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected internal documentation and determined vulnerabilities were classified based on the priority level.	No deviations noted.
	Inspected relevant configurations and determined vulnerabilities were tracked through an internal ticketing system as outlined in the vulnerability management program.	No deviations noted.
	Inspected a sample of identified vulnerabilities and determined they were tracked in an internal ticketing system through remediation.	No deviations noted.
6. The organization has established a process to review and approve requests for policy exceptions.	Inquired of the Program Manager and determined Google has a policy exception process to ensure a formal approval and risk evaluation are performed.	No deviations noted.
	Inspected applicable policies and determined the process to request and process policy exceptions was documented.	No deviations noted.
	Inspected a sample of policy exceptions and determined they followed the process as described in the policy.	No deviations noted.
7. The organization requires external parties (Service Providers) to meet security and privacy requirements for safeguarding user data. Requirements are enforced via the “Information Protection Addendum (IPA)” or “Partner Information Protection Addendum (PIPA)” for	Inquired of the Program Manager and determined the organization required external parties (Service Providers) to meet security and privacy requirements for safeguarding user data and the requirements were enforced via the “Information Protection Addendum (IPA)” or “Partner Information Protection Addendum (PIPA)” for providers and partners, respectively.	No deviations noted.
	Inspected relevant documentation and determined the organization had a formal due diligence process in place for engaging with third parties.	No deviations noted.

bernard@hotmaker.io

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
vendors/service providers and partners, respectively.	Inspected the Information Protection Addendum (IPA) template and determined appropriate information security and data protection terms were documented within the IPA.	No deviations noted.
	Inspected the Partner Information Protection Addendum (PIPA) template and determined appropriate information security and data protection terms were documented within the PIPA.	No deviations noted.
	Inspected a sample Vendor that processes Google customer data and determined that they had signed an Information Protection Addendum (IPA) or Partner Information Protection Addendum (PIPA).	No deviations noted.
8. The organization tests, validates, and documents changes to its services prior to deployment to production.	Inquired of the Program Manager and determined that application and configuration changes are tested, validated, and documented prior to deployment to production.	No deviations noted.
	Inspected the associated ticket details for a sample of Google Cloud Platform application and configuration changes in the code management system and determined that the changes were tested, validated, and documented prior to implementation to production.	Deviations Noted. For four (4) samples of the seventy-five (75) sampled changes selected for testing, documentation was not retained to evidence the testing performed in the staging environment prior to deployment to production.

hemant@bottomline.in

Google Confidental Information

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Management's response: Management acknowledges that four (4) selected sample changes lacked evidence of testing conducted in the staging environment prior to production deployment. Although the control process over testing of changes prior to deployment is common across different Google products, management identified that the 4 impacted sample changes were not related to Google Cloud products. Management also determined that these changes were tested in the staging environment, but evidence of this testing was not subsequently recorded in the test log. Further, management performed a comprehensive review of the 4 changes and determined that the changes were valid, with no impact on production resources. Two (2) of the changes involved parameter adjustments to open-source code, and the remaining two (2) were minor database configuration updates. Management reiterated the importance of following change management policies to ensure that changes are tested and documented prior to production deployment. Additionally, management identified the four changes were validated and approved by a second engineer prior to production deployment as tested in Control 8 in CO3 of the report.	
	Inspected the associated ticket details for a sample of Google Cloud Platform application and configuration changes in the code management system and determined that the changes were tested, validated, and documented prior to implementation to production.	No deviations noted.
9. The organization has established a privacy and information security training	Inquired of the Program Manager and determined privacy and information security training program was in place and relevant personnel were required to complete this training annually.	No deviations noted.

bernard@dotmaker.ie

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
program and requires relevant personnel to complete this training annually.	Inspected internal documentation and determined privacy and information security training program was in place and relevant personnel were required to complete the training annually.	No deviations noted.
	Inspected a sample email notification sent to Google personnel and determined reminders were sent to complete the privacy and information security training within a specified time.	No deviations noted.
	Inspected the completion rate for the privacy and information security training for Google personnel and determined relevant personnel completed the trainings in the last 12 months or were actively being monitored until completion of training.	No deviations noted.
	Inspected the privacy and information security training material and determined that Google has outlined the importance of information security and maintaining user, customer and employee privacy.	No deviations noted.
	Inspected the continuing education documents and determined that the entity provided training programs to help ensure skill sets and technical competencies of existing employees and contractors were developed and maintained.	No deviations noted.
	Inspected the training activity dashboard and determined that the privacy and information security training was mandatory and required to be completed annually.	No deviations noted.

hernan@bernake.ro

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
10. The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inquired of the Program Manager and determined the organization conducted periodic information security risk assessments to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No deviations noted.
	Inspected applicable documentation and determined a risk management framework was developed and documented to manage risk to an acceptable level and defined resolution time frames for risks.	No deviations noted.
	Inspected the risk assessment and determined the organization conducted periodic information security risk assessments and identified, evaluated and mitigated risks to acceptable levels based on risk criteria, which are established, documented and approved by management.	No deviations noted.
	Inspected the organization's risk assessment and determined management signed off on the annual risk assessments performed.	No deviations noted.
11. The organization develops and maintains a risk management framework to manage risk to an acceptable level.	Inquired of the Program Manager and determined the organization developed and maintained a risk management framework to manage risk to an acceptable level.	No deviations noted.
	Inspected the vulnerability management and severity guidelines and determined a risk management framework was developed and documented to manage risk to an acceptable level, defined resolution time frames for risks, and to consider the potential for fraud.	No deviations noted.

kernel@botmaker.io

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected internal documentation and determined the organization maintains a security risk assessment framework to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented and signed off by management.	No deviations noted.
	Inspected the organization's risk assessment and determined the organization evaluates qualitative and quantitative factors to identify residual risk in order to manage risk to an acceptable level.	No deviations noted.
	Inspected meeting invites and relevant documentation from the organization's annual risk assessment discussion and determined the organization's operational objectives, potential impacts, and changes to the business model were considered.	No deviations noted.
	Inspected the internal insider risk site and determined the organization considered insider risk in its risk management framework to manage risk to an acceptable level.	No deviations noted.
12. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by management.	Inquired of the Program Manager and determined the organization conducted periodic information security risk assessments to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No deviations noted.
	Inspected applicable documentation and determined a risk management framework was developed and documented to manage risk to an acceptable level and defined resolution time frames for risks.	No deviations noted.

bernardoatmaker.no

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected the risk assessment and determined the organization conducted periodic information security risk assessments and identified, evaluated and mitigated risks to acceptable levels based on risk criteria, which are established, documented and approved by management.	No deviations noted.
	Inspected the organization's risk assessment and determined management signed off on the annual risk assessments performed.	No deviations noted.
13. The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inquired of the Program Manager and determined the organization requires its employees to sign confidentiality agreements that define responsibilities and expected behavior for the protection of information.	No deviations noted.
	Inspected a sample of confidentiality agreements and determined they defined employee responsibilities and expected behavior for the protection of information.	No deviations noted.
	Inspected a sample of the organization's employees and determined they signed confidentiality agreements as part of their employment conditions.	No deviations noted.

bernard@dnamaker.io

Google Confidental Information

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inquired of management and determined if any control deviations were identified during their own internal testing procedures.	Deviation noted. Per review of the first party audit report, for one (1) of thirty-four (34) sampled employees, we determined that the confidentiality agreement was not signed timely for a sample employee.
	Management's Response: Management acknowledges and accepts the audit finding identified as part of the first party audit regarding the Confidential Information and Invention Assignment Agreement (CIIAA) not being signed prior to employment for 1 out of 34 employees. Management has remediated the finding related to the impacted sample employee by having the CIIAA signed by the employee upon discovery of the incident. Additionally, EY performed additional independent testing for a random sample of 25 employees and no deviations were identified. As a result, management determined the finding was related to an isolated incident.	
14. Personnel of the organization are required to acknowledge the code of conduct.	Inquired of the Program Manager and determined employees and extended workforce personnel were required to acknowledge the Code of Conduct as part of the terms and conditions of employment.	No deviations noted.
	Inspected internal documentation and determined employees and extended workforce personnel were required to acknowledge the Code of Conduct as part of the terms and conditions of employment.	No deviations noted.

bernard@gotmaker.io

Google Confidental Information

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected a sample of newly hired employees and extended workforce personnel and determined the Code of Conduct was acknowledged as part of the terms and conditions of their employment.	Deviation noted. For one (1) of twenty-five (25) sampled employees we determined that the code of conduct was not signed timely.
	Management's Response: Management acknowledges and accepts the audit finding regarding the code of conduct not being signed within 5 weeks from the start date for one (1) sample employee out of twenty-five (25). Management noted that the code of conduct was acknowledged by the impacted sampled employee after 8 weeks of the start date (November 18, 2024) noting that the root cause of the delay on signing of the code of conduct was because the initiation of the Code of Conduct task was dependent on the employee's completion of the required onboarding steps as part of the onboarding checklist. Management reviewed the impacted employee's onboarding checklist and determined that the employee completed the required onboarding steps except for the tax withholding submission on November 18, 2024. The tax withholding submission step was completed by the employee on December 9, 2024, which then triggered the Code of Conduct task that was subsequently completed on January 3, 2025. Additionally, the required onboarding steps were appropriately tracked within the checklist and that the employee's hiring manager was appropriately informed of the series of events from the start of the employee's onboarding process up to its completion. As a result of the designed onboarding process dependencies, management determined the delay was due to an upstream process step and was not due to the failure of the control governing Code of Conduct acknowledgment once initiated.	

bernard@gradmaker.io

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
15. Company goals and responsibilities are required to be developed and communicated by management on a periodic basis, and amended as needed. Results are evaluated and communicated to employees.	Inquired of the Program Manager and determined company goals and responsibilities were developed and communicated by management and amended as needed. Results of the annual goals were evaluated and communicated to employees.	No deviations noted.
	Inspected a sample of annual objectives and key results and determined company goals and responsibilities were developed and communicated by management.	No deviations noted.
	Inspected a sample announcement and determined results of previous goals were communicated to employees.	No deviations noted.
16. New hires or internal transfers are required to go through an official recruiting process during which they are screened against detailed job descriptions and interviewed to assess competence.	Inquired of the Program Manager and determined that new hires and internal transfers were required to go through an official recruiting process during which their qualifications and experience were screened against detailed job descriptions to help ensure that they were competent to fulfill their responsibilities.	No deviations noted.
	Inspected relevant internal hiring guidelines and determined that the organization has implemented an official recruiting process for new hires and internal transfers.	No deviations noted.
	Inspected a sample of new hires and internal transfers and determined positions had detailed job description including minimum and preferred qualifications, such as requisite skills and experiences, which candidates must meet in order to be hired.	No deviations noted.

hernandehotmail.io

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected a sample of new hires and internal transfers and determined they went through a formal recruiting process and were screened against detailed job descriptions and interviewed to assess competence.	No deviations noted.
17. Background checks are performed on new hires as permitted by local laws.	Inquired of the Program Manager and determined background checks were performed for new hires as permitted by local laws.	No deviations noted.
	Inspected internal guidelines and determined background checks were part of the hiring process.	No deviations noted.
	Inspected a sample of new hires and determined background checks were performed as permitted by local laws.	No deviations noted.
18. The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inquired of the Program Manager and determined the organization had established agreements, including non-disclosure agreements, for preserving confidentiality of information and software exchanges with external parties, such as third-party vendors.	No deviations noted.
	Inspected relevant documentation and determined the organization had established agreements in place, including non-disclosure agreements, for preserving confidentiality of information and software exchanges with external parties, such as third-party vendors.	No deviations noted.
	Inspected the latest non-disclosure agreement template and determined the organization had established agreements with external parties for preserving confidentiality of information and software exchanges.	No deviations noted.

bernard@tomaker.io

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected agreements for a sample of external parties and determined the organization had signed non-disclosure agreements for preserving confidentiality of information and software exchanges with external parties.	No deviations noted.
19. The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inquired of the Program Manager and determined the organization required its extended workforce personnel to sign confidentiality agreements that defined responsibilities and expected behavior for the protection of information.	No deviations noted.
	Inspected the organization's confidentiality agreements and determined they defined extended workforce personnel responsibilities and expected behavior for the protection of information.	No deviations noted.
	Inspected a sample extended workforce personnel and determined they signed the confidentiality agreements, indicating their acceptance of the responsibilities and expected behavior in regards to protection of information.	No deviations noted.
20. The organization periodically reviews and validates the design, operation and control record of in-scope compliance controls.	Inquired of the Program Managers and Internal Audit and determined that the organization had an established internal compliance function which periodically evaluates, reviews and validates the design, operation and management's compliance with security and privacy controls.	No deviations noted.
	Inspected evaluations performed by the internal compliance function for a sample of semiannual periods and determined that the compliance function performed an evaluation of management's compliance with security and privacy controls.	No deviations noted.

bernard@riskmarket.io

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected evaluations performed by management for a sample of quarters and determined that management performed an evaluation of their compliance with security and privacy controls.	No deviations noted.
	Inspected the meeting invites related to the organization's annual organizational risk assessment and determined that the company's operational objectives, and potential impacts and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.
21. The organization performs privacy reviews prior to product launch.	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.
	Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
	Inspected a sample product launch and determined a design document and privacy review were completed prior to the launch.	No deviations noted.
	Inspected a sample of official product blogs for product and feature releases and determined relevant personnel and impacted customers were notified.	No deviations noted.

bernardoramos.pt

Google Confidental Information

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
22. Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inquired of the Program Manager and determined security and privacy policies are reviewed at least annually, and supporting standards, guidelines, and FAQs are created and updated as needed.	No deviations noted.
	Inspected internal documentation and determined that security and privacy policies, supporting standards, guidelines and FAQS were in place.	No deviations noted.
	Inspected internal documentation and determined security and privacy policies were reviewed at least annually and authorized before they were implemented.	No deviations noted.
	Inspected the most recent security and privacy policy reviews and determined policies were approved by authorized personnel or committee, reviewed at least annually, and updated as needed.	No deviations noted.
23. The Privacy, Safety Security Org (PSS) takes a risk based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	Inquired of the Program Manager and determined that the Privacy, Safety Security Org (PSS) takes a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	No deviations noted.
	Inspected the relevant documentation and determined the Privacy, Safety Security Org (PSS) took a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products, including automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	No deviations noted.

hernan@bartmaker.io

Google Confidental Information

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected a sample of vendors and determined the security practices of vendor and the security posture of vendor products were reviewed.	No deviations noted.
24. Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.
	Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
	Inspected a sample product launch and determined a design document and privacy review were completed prior to the launch.	No deviations noted.
	Inspected a sample of official product blogs for product and feature releases and determined relevant personnel and impacted customers were notified.	No deviations noted.
25. The organization has an established Internal Audit function which evaluates management's compliance with security controls.	Inquired of the Program Managers and Internal Audit and determined that the organization had an established internal compliance function which periodically evaluates, reviews and validates the design, operation and management's compliance with security and privacy controls.	No deviations noted.

kermani@batmail.c

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected evaluations performed by the internal compliance function and determined that the compliance function performed an evaluation of management's compliance with security and privacy controls.	No deviations noted.
	Inspected evaluations performed by management for a sample of quarters and determined that management performed an evaluation of their compliance with security and privacy controls.	No deviations noted.
	Inspected the meeting invites related to Google's annual organizational risk assessment and determined that the company's operational objectives, and potential impacts and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.
26. The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Inquired of the Program Manager and determined Google published its commitments to security, availability, processing integrity and confidentiality to external users via Terms of Service (ToS).	No deviations noted.
	Inspected Google Cloud Platform's Terms of Service and product websites and determined Google's commitments to security, availability, processing integrity, and confidentiality are published for external users.	No deviations noted.

bo.gardner@trackt.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
1. The organization has a security guideline that requires users to lock their workstations and mobile devices when unattended. Workstations are configured to initiate a password protected screen-saver after 15 minutes of inactivity (i.e., no input from device user).	Inquired of the Program Manager and determined a security guideline was in place that required users to lock workstations and mobile devices when unattended.	No deviations noted.
	Inspected internal policies and determined the organization required users to lock their workstations and mobile devices when unattended.	No deviations noted.
	Inspected the idle time configurations propagated to workstations and determined they were configured to enforce password standards.	No deviations noted.
	Performed on-site inspections for a sample of offices and determined that employees followed appropriate office security practices including locking workstations when unattended.	No deviations noted.
	Observed a sample of corporate machines and determined users were locked out after reasonable amount of time of inactivity.	No deviations noted.
2. The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	Inquired of the Program Manager and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	No deviations noted.
	Inspected the internal documentation and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the network	No deviations noted.

beardedpotpoker.com

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
3. Personnel access to internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	Inquired of the Program Manager and determined access to sensitive systems and applications requires two-factor authentication in the form of user ID, password, security key, and/or certificate.	No deviations noted.
	Inspected the applicable policy and determined access to sensitive systems and applications required two-factor authentication in the form of user ID, password, security key and/or certificate.	No deviations noted.
	Inspected relevant policy documentation and determined the organization has an established policy that specifies the use of emergency credentials.	No deviations noted.
	Inspected the configuration and determined that personnel access to sensitive internal systems and applications required two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	No deviations noted.
	Observed a user attempt to gain access to a production machine with a valid user ID, password, security key, and certificate and determined access was granted.	No deviations noted.
	Observed a user attempt to gain access to a production machine without a valid certificate and determined access was not granted.	No deviations noted.
	Observed a user attempt to gain access to a production machine with valid emergency access credentials and determined access was granted.	No deviations noted.

bernard@bitmaker.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Observed a user attempt to gain access to a production machine without valid emergency access credentials and determined access was not granted.	No deviations noted.
4. Security event logs are protected and access is restricted to authorized personnel.	Inquired of the Program Manager and determined security event logs were protected and access was restricted to authorized personnel.	No deviations noted.
	Inspected internal documentation and determined policies and procedures for restriction of logical access to audit logs to authorized personnel were in place.	No deviations noted.
	Inspected the system code related to audit logs and determined log files are frozen and access to modify logs is restricted	No deviations noted.
	Inspected a sample of members with access to audit logs and determined they were appropriate to have access to audit logs.	No deviations noted.
	Inspected a sample semiannual user access review and determined access to audit logs was reviewed on a periodic basis and that appropriate action was taken to resolve inappropriate access, if applicable.	No deviations noted.
5. Remote access to corporate machines requires a digital certificate issued by the organization installed on the connecting device, and two-factor	Inquired of the Program Manager and determined remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate.	No deviations noted.

bernard@bothmaker.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
authentication in the form of user ID, password, security key, and/or certificate.	Inspected relevant documentation and determined remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificates.	No deviations noted.
	Inspected the remote access configuration and determined it required a Company issued digital certificate to be installed on the connecting device.	No deviations noted.
	Inspected the authentication settings for remote access to corporate machines and determined two-factor authentication was required.	No deviations noted.
	Observed a user attempt to gain remote access to corporate machine with a device that had a Company issued digital certificate installed and two-factor authentication and determined remote access to the corporate environment was successful.	No deviations noted.
	Observed a user attempt to gain remote access to corporate machine with a device that did not have a Company issued digital certificate installed and determined remote access to the corporate environment was denied.	No deviations noted.
	Observed a user attempt to gain remote access to corporate machine with a device without two-factor authentication and determined remote access to the corporate environment was denied.	No deviations noted.

bernard@batmaker.io

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
6. Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	Inquired of the Program Manager and determined that access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists were recorded and approved by administrators.	No deviations noted.
	Inspected relevant documentation and formal procedures for managing user access to production machines, support tools, and network devices via access control lists and determined that access requests and modifications must be recorded and approved by appropriate administrators.	No deviations noted.
	Inspected the configurations within the source code management system and determined that the relevant access control list systems were configured to enforce approval from a group administrator prior to a user receiving access to production machines, support tools, and network devices.	No deviations noted.
	Observed an attempt to grant user access to a group with the appropriate approval from the group administrator and determined access was granted.	No deviations noted.
	Observed an attempt to grant user access to a group without the appropriate approval from the group administrator and determined access was not granted.	No deviations noted.
	Inspected a sample of system generated logs for access to production machines, support tools, and network devices and determined access approvals and modifications to the access lists were recorded.	No deviations noted.

bernard@ottiker.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
7. Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.	Inquired of the Program Manager and determined access to the corporate network, which further provides access to production machines, network devices, and support tools, required a unique ID, password, valid credentials, and/or machine certificates.	No deviations noted.
	Inspected the configuration for access to corporate network, network devices, production machines, and support tools and determined a unique ID, password, valid credentials, and/or machine certificates were required.	No deviations noted.
	Observed a user attempt to create a user with a username belonging to another user and determined that a duplicate username could not be assigned.	No deviations noted.
	Observed a user attempt to create, delete, and recreate an account with the same username and determined the accounts were assigned unique IDs.	No deviations noted.
	Observed a user attempt to access the corporate network without valid credentials and determined access was denied.	No deviations noted.
	Observed a user attempt to access the corporate network with valid credentials and determined access was granted.	No deviations noted.
	Observed a user attempt to access the production machines with an authorized private key by using a valid SSH certificate and determined access was allowed.	No deviations noted.

bernard@bonneau.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Observed a user attempt to access the production machines without an authorized private key by using an invalid SSH certificate and determined access was denied.	No deviations noted.
	Observed a user attempt to obtain access to network devices after authenticating via user ID, password, security key, and/or certificate and determined that the user successfully obtained access.	No deviations noted.
	Observed a user attempt to obtain access to network devices without first authenticating via user ID, password, security key, and/or certificate and determined that the user failed to obtain access.	No deviations noted.
	Observed a user attempt to access an internal support tool with valid credentials and determined access was granted.	No deviations noted.
	Observed a user attempt to access an internal support tool without valid credentials and determined access was not granted.	No deviations noted.
	Observed an engineer attempt to request a certificate and determined the key management process was followed to support the organization's internal and external use of cryptographic techniques.	No deviations noted.
	Inspected a sample of internal and external certificate revocation requests and determined certificates were revoked timely.	No deviations noted.

b4nan@batmaker.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
8. Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.	Inquired of the Program Manager and determined access to network devices was authenticated via user ID, password, security key, and/or certificate.	No deviations noted.
	Inspected the access configuration for production network devices and determined it required authentication via user ID, password, security key, and/or certificate.	No deviations noted.
	Observed a user attempt to obtain access to network devices after authenticating via user ID, password, security key, and/or certificate and determined that the user successfully obtained access.	No deviations noted.
	Observed a user attempt to obtain access to network devices without first authenticating via user ID, password, security key, and/or certificate and determined that the user failed to obtain access.	No deviations noted.
9. The organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inquired of the Program Manager and determined the organization had established password guidelines to govern the management and use of authentication mechanisms.	No deviations noted.
	Inspected relevant documentation and determined formal guidelines for passwords were established to govern the management and use of authentication mechanisms.	No deviations noted.
	Inspected the relevant configurations and determined passwords were transmitted and stored in an encrypted manner.	No deviations noted.

hernan@bottmaker.ro

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the password configurations propagated to servers and determined they were configured to enforce password requirements.	No deviations noted.
	Observed user attempt to login using incorrect password and determined the account was locked out after exceeding the maximum number of attempts allowed.	No deviations noted.
10. Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Inquired of the Program Manager and determined that critical access groups were reviewed on a periodic basis by group administrators and inappropriate access was removed.	No deviations noted.
	Inspected relevant documentation and determined that critical access group reviews were done on a periodic basis and scoping was determined accordingly.	No deviations noted.
	Inspected the code configuration and determined that tools used to facilitate the review generated complete and accurate critical access group listings semi-annually and assigned the group administrators.	No deviations noted.
	Inspected a sample of critical access group user membership reviews performed by the appropriate group administrator and determined the review was performed in a timely manner.	Deviations noted. Four (4) of fifty-three (53) critical access groups in the semi-annual review sampled for testing were not performed timely.

bannerbatmaker.io

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Management's Response: Management acknowledges that the periodic access review for 4 selected critical access group was not performed in a timely manner and completed after the defined service level objective (SLO). Management reviewed the memberships to the access groups and determined that there was no inappropriate access identified as result of the delayed review. As per Google's policy, the defined SLO for a review to be completed is 42 days. Reminders are automatically sent to the reviewer at 5, 12, 25, 35, and 41 days. After 25 days, the reviewer's manager is copied on the reminders. If the 42-day SLO has passed, the priority of the review ticket is updated to the highest engineering priority. Management has reiterated the importance of timely completion of the user access reviews to the relevant teams to ensure that reviews are completed within the defined SLO. In addition, the Google security compliance team makes training materials and process documentation readily available to all Google employees.	
	Inspected a sample of users from the review of critical access groups and determined their access was appropriate based on their cost center.	No deviations noted.
	Inspected a sample critical access group user membership review and determined that appropriate action was taken to resolve inappropriate access identified, if applicable.	No deviations noted.

bernardsbotmaker.io

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected a sample critical access group review and determined they reviewed a complete and accurate listing of critical access groups.	Deviations noted. For twenty-three (23) groups impacting twenty-four (24) products with access to approve or deploy changes to production, were not tagged as critical access groups, hence, were not included in management's review of critical access groups.
	Management's Response: Management reviewed the findings related to the 23 critical access groups for the 24 products that were not included in the periodic access review process, noting the root cause to be an omission resulting from manual error. Management reviewed the memberships to the access groups that were not formally included in the periodic access review process and determined that there was no inappropriate access identified. Further, management has added the 21 of the 23 impacted access groups to the ongoing periodic critical access group review process. For the remaining two (2) impacted groups, key access permissions to edit or write code were removed, hence, would not be tagged as critical access groups. Additionally, Management has assigned compliance specialists to partner with each of the product teams in scope on the design, implementation and testing of security controls. These compliance specialists review the internal control details associated with these products at least annually, with ad hoc reviews as necessary.	

bernard@botmaker.io

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected a sample critical access group user membership review and determined the review was automatically generated semi-annually.	No deviations noted.
	Inspected a sample critical access group user membership review and determined the review was automatically assigned to a random group owner, the remaining owners were CC'ed and a review link was provided.	No deviations noted.
	Inspected a sample critical access group user membership review and determined a reminder was automatically generated for an incomplete review.	No deviations noted.
	Inspected a sample critical access group user membership review and determined that when the review was completed within the front-end UI tool provided, the review ticket automatically closed.	No deviations noted.
	Inspected a sample critical access group user membership review and determined the review was automatically assigned to a random Eng Compliance Business Partner if the group owner was unable to be found.	No deviations noted.
11. Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis upon submission of a	Inquired of the Program Manager and determined access to production machines, support tools, network devices and corporate assets was automatically removed on a timely basis upon submission of a termination request by Human Resources or a manager.	No deviations noted.

hernan@botmaker.co

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
termination request by Human Resources or a manager.	Inspected relevant documentation and determined requirements for terminating users with access to production machines, support tools, network devices and corporate assets were documented.	No deviations noted.
	Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined it was configured to remove access upon submission of a termination request by Human Resources or a manager.	No deviations noted.
	Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined that any failures in the process will generate an alert.	No deviations noted.
	Inspected a sample alert from the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined that the failure was resolved in a timely manner.	No deviations noted.
	Inspected a sample of terminated users and determined that access to production machines, support tools, network devices, and corporate assets was automatically revoked by the automated tool within seven (7) days of the user's termination date.	No deviations noted.
12. Only users with a valid user certificate, corresponding private key and appropriate authorization	Inquired of the Program Manager and determined only users with a valid certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	No deviations noted.

bernardoolmedo.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
(per host) can access production machines via SSH.	Inspected relevant documentation and determined mechanisms are in place to authenticate users and restrict access to production machines without a valid digital certificate.	No deviations noted.
	Inspected the configuration that enforced the authentication of users prior to granting a private key and determined digital certificates were only generated after a user was authenticated using two-factor authentication.	No deviations noted.
	Inspected a user attempt to access the production machines with an authorized private key by using a valid SSH certificate and determined access was allowed.	No deviations noted.
	Inspected a user attempt to access the production machines without an authorized private key by using an invalid SSH certificate and determined access was denied.	No deviations noted.
13. Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	Inquired of the Program Manager and determined access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No deviations noted.
	Inspected the configuration and determined access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No deviations noted.
	Inspected a user attempt to access an internal support tool with approved credentials and determined access was granted.	No deviations noted.
	Inspected a user attempt to access an internal support tool without approved credentials and determined access was not granted.	No deviations noted.

bernard@batmaker.io

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
14. Mechanisms are in place to detect attempts, and prevent connections to the organization's network by unauthorized devices.	Inquired of the Program Manager and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
	Inspected relevant documentation and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
	Inspected relevant configurations and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
	Observed a user with an authorized device attempt to connect to the organization's network and determined the connection was successful.	No deviations noted.
	Observed an unauthorized user attempt to connect to the organization's network and determined access was denied.	No deviations noted.
	Observed a user attempt to connect to the production network with a valid certificate and determined the connection was successful.	No deviations noted.
	Observed a user attempt to connect to the production network without a valid certificate and determined that access was denied.	No deviations noted.
	Observed a user modify their certificate and determined that access was disconnected.	No deviations noted.

bernard@bottmaker.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected a sample alert and determined mechanisms were in place to detect attempts at unauthorized connections to the organization's network.	No deviations noted.
15. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	Inquired of the Program Manager and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
	Inspected internal policies regarding encryption mechanisms and determined the organization used encryption to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
	Inspected externally available documentation and determined the organization communicated how user authentication and administrator sessions transmitted over the Internet were encrypted.	No deviations noted.
	Inspected encryption mechanism documentation and configurations, and determined user authentication and administrator sessions transmitted over the Internet were encrypted.	No deviations noted.
	Observed connection settings to the organization's external websites for a user and an administrator and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.

hernan@bottmaker.ro

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the server scan results and determined the organization used encryption mechanisms to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
16. External system users are identified and authenticated via the Google Accounts or the BYOID authentication system before access is granted.	Inquired of the Program Manager and determined external system users were identified and authenticated via the organization's authentication system before access is granted.	No deviations noted.
	Inspected the configuration supporting the login functionality and determined users were identified and authenticated via the organization's authentication system before access was granted.	No deviations noted.
	Observed an external system user login with a valid organizational account and determined access was granted.	No deviations noted.
	Observed an external system user attempt to login with an invalid organizational account and determined access was denied.	No deviations noted.
17. The organization uses encryption to secure user data in transit between the organization's production facilities.	Inquired of the Program Manager and determined the organization used encryption to secure user data in transit between production facilities.	No deviations noted.
	Inspected internal documentation and determined encryption was used to secure user data in transit between the organization's production facilities.	No deviations noted.

bernard@bernard.io

Google Confidental Information

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the encryption configuration and determined encryption was used to secure user data in transit between the organization's production facilities.	No deviations noted.
18. Where "on demand request" mechanisms are implemented to restrict human access to production resources, access requests are reviewed and approved by a second individual prior to being granted and the event is logged.	Inquired of the Program Manager and determined that "on demand request" mechanisms are implemented to restrict human access to production resources, and "access on demand" requests are reviewed and approved by a second individual prior to being granted and the event is logged.	No deviations noted.
	Inspected relevant documentation and determined that "access on demand" requests are reviewed and approved by an appropriate second individual prior to being granted and that the event is logged.	No deviations noted.
	Inspected the "access on demand" configuration supporting the functionality and determined access requests are configured to restrict human access to production resources via access groups and can only be granted for a limited number of hours.	No deviations noted.
	Observed a user attempt to gain access to an on-demand group and determined access was granted after meeting the predefined conditions (i.e., authorized user request, appropriate approval from a second individual, limited number of hours).	No deviations noted.
	Observed a user attempt to gain access to an on-demand group and determined access was not granted when the predefined conditions (i.e., authorized user request, appropriate approval from a second individual, limited number of hours) were not met.	No deviations noted.

bernard@kanmaker.io

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected a sample of system generated logs and determined that on-demand group transactions were recorded.	No deviations noted.

bernard@botmaker.io

Google Confidental Information

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
1. Development, testing and build environments are separated from the production environment through the use of logical security controls.	Inquired of the Program Manager and determined the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
	Inspected internal documentation and determined the organization maintained separate development, testing, and production environments.	No deviations noted.
	Inspected the relevant code and determined that builds deployed into production are systematically verified prior to deployment or have a valid exception.	No deviations noted.
	Observed that manual builds must still be submitted, reviewed and systematically verified prior to deployment to production.	No deviations noted.
	Inspected security and access restriction settings for a sample of products related to the change pipeline for services running in the organization's production environment, and determined that the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
	Inspected security and access restriction settings for a sample of products related to the change pipeline for open source code packages maintained in a public source code repository, and determined that the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.

kenan@patmarr.io

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected security and access restriction settings for a sample of products related to the change pipeline for images, downloads, or software updates made available to customers, and determined that the organization separated development, testing, and build environments from production through the use of logical security controls.	Deviation noted. For three (3) of fifty-eight (58) products sampled for testing, sixteen (16) users with admin/write access within development, testing, and build registries prior to deployment were not added to either critical access groups (CAGs) or on-demand groups. As such, users were not controlled through the use of logical security controls governing CAGs and on-demand groups.

bernard@botmaker.io

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Management's Response: Management acknowledges that for 3 identified products, 16 users had direct access to resources within the software deployment process, such as build repositories. Although the control process over separation of development, testing, and build environments from production through the use of logical security controls is common across different Google products, management identified that the two (2) of the three (3) impacted sample products changes were related to Apigee and Data products. The remaining one (1) product is not related to Google Cloud Platform. Management determined that access to these resources is expected to be provided through critical access groups (CAGs) or on-demand groups. This deviation occurred as a result of teams incorrectly provisioning access at the user level rather than the group level and was an oversight. Further, management conducted a comprehensive review of users with access to these resources and direct user access has been revoked. The direct user access had not resulted in unauthorized changes to production and there was no impact to production resources. Access has been appropriately restricted to designated groups which are managed as a part of Google's established access control procedures. Additionally, management noted that Control 8 in CO3 of the report related the enforcement of multi-party approval for code changes would further mitigate the risk associated with this finding.	
	Inspected a sample Google Cloud Platform change and determined the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
2. The organization has policies and guidelines governing the secure development lifecycle.	Inquired of the Program Manager and determined the organization had policies and procedures which govern the secure development lifecycle.	No deviations noted.

benefits@stmarys.ca

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected internal documentation and determined the organization had policies and procedures which govern the secure development lifecycle.	No deviations noted.
3. The organization has a published policy about retention and deletion of user data.	Inquired of the Program Manager and determined Google has a User Data Retention and Deletion Policy.	No deviations noted.
	Inspected the User Data Wipeout Policy and other related documentation, and determined they established guidelines to govern the retention and deletion of user data.	No deviations noted.
4. The organization has established guidelines for governing the installation of software on organization-owned assets.	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
	Inspected the organization's security policies and determined the organization had implemented rules to govern the installation of software by users.	No deviations noted.
	Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.

bernardbaker.io

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
	Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.
	Inquired of the Program Manager and determined that a standard production image was utilized for the installation and maintenance of each production server.	No deviations noted.

bernard@ahmed.io

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected a sample configuration of the tool the organization uses to monitor the virtual machines and detection of deviations for the virtual machine.	No deviations noted.
	Inspected a sample of tickets and determined that deviations identified in virtual machines are detected and corrected.	No deviations noted.
5. The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Inquired of the Program Manager and determined change management policies, including security code reviews, were in place, and procedures for tracking, testing, approving, and validating changes were documented.	No deviations noted.
	Inspected internal policies and determined practices for security code review, tracking, testing, approving, and validating changes were documented.	No deviations noted.
6. The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inquired of the Program Manager and determined the organization used an internal code management system to manage source code, documentation, release labeling, and that access to the system has to be approved.	No deviations noted.
	Inspected internal documentation and determined the organization uses a version control system, to manage source code, documentation, release labeling, and other functions.	No deviations noted.
	Inspected code change management tools and determined that there was a version control system in place to manage source code, code documentation, and release labeling.	No deviations noted.

bernard@bolnaker.io

Google Confidental Information

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the system configurations for the code management system and determined the system was configured to require an approval prior to granting access to the version control system.	No deviations noted.
7. Changes to the organization's systems are tested before being deployed.	Inquired of the Program Manager and determined that application and configuration changes are tested, validated, and documented prior to deployment to production.	No deviations noted.
	Inspected the associated ticket details for a sample of product application and configuration changes related to services running in the organization's production environment, and determined that the changes were tested, validated, and documented prior to implementation to production.	No deviations noted.
	Inspected the associated ticket details for a sample of product application and configuration changes related to open source code packages maintained in a public source code repository, and determined that the changes were tested, validated, and documented prior to implementation to production.	Deviations noted. For four (4) samples of the twenty-five (25) sampled changes selected for testing, documentation was not retained to evidence the testing performed in the staging environment prior to deployment to production.

bernard@drata.io

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Management's Response: Management acknowledges that four (4) selected sample changes lacked evidence of testing conducted in the staging environment prior to production deployment. Although the control process over testing of changes prior to deployment is common across different Google products, management identified that the 4 impacted sample changes were not related to Google Cloud products. Management also determined that these changes were tested in the staging environment, but evidence of this testing was not subsequently recorded in the test log. Further, management performed a comprehensive review of the 4 changes and determined that the changes were valid, with no impact on production resources. Two (2) of the changes involved parameter adjustments to open-source code, and the remaining two (2) were minor database configuration updates. Management reiterated the importance of following change management policies to ensure that changes are tested and documented prior to production deployment. Additionally, management identified the four changes were validated and approved by a second engineer prior to production deployment as tested in Control 8 in CO3 of the report.	
	Inspected the associated ticket details for a sample of product application and configuration changes related to images, downloads, or software updates made available to customers, and determined that the changes were tested, validated, and documented prior to implementation to production.	No deviations noted.
8. System changes are reviewed and approved by a separate	Inquired of the Program Manager and determined system changes were reviewed and approved by a separate technical resource before migration to production.	No deviations noted.

bernardo@tmanage.me

Google Confidental Information

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
technical resource before moving into production.	Inspected the applicable code for the organization's code management system and determined system changes required a review by a separate technical resource before migration to production.	No deviations noted.
	Inspected evidence of transaction testing made by a user to the version code management system and determined that it required changes to be reviewed by a separate technical resource before migration to production.	No deviations noted.
9. Changes to network configurations are reviewed and approved prior to deployment.	Inquired of the Program Manager and determined changes to network configurations were reviewed, approved, and tested prior to deployment.	No deviations noted.
	Inspected a sample of manual network configuration changes and determined they were reviewed by a separate technical resource to validate quality and accuracy.	No deviations noted.
	Inspected a sample of manual network configuration changes and determined they were tested prior to deployment.	No deviations noted.
	Inspected a sample automated change and determined it was made by an automated tool based on the pre-configured ruleset.	No deviations noted.
	Inspected a sample of changes made to the automated tool and determined it was reviewed by a separate technical resource to validate quality and accuracy and tested prior to deployment.	No deviations noted.

bernard@rentmaker.io

Google Confidental Information

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
10. Mobile code is blocked by default via standard (Chrome) web browser configurations on company owned endpoints.	Inquired of the Program Manager and determined mobile code (code that is executed in a remote location) is blocked by default via standard web browser configurations on Google workstations and laptops.	No deviations noted.
	Inspected relevant documents and policies for configuration of the standard web browser (Chrome) on Google workstations and laptops and determined the organization implemented rules to restrict unauthorized portable code.	No deviations noted.
	Inspected relevant code configurations and determined rules were configured to block code via standard web browser (Chrome) configurations.	No deviations noted.
	Observed a standard web browser (Chrome) and determined blocked extensions/domains could not be accessed.	No deviations noted.
11. A standard image is utilized for the installation and maintenance of each production server.	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
	Inspected Google's security policies and determined Google had implemented rules to govern the installation of software by users.	No deviations noted.

bernard@mathaker.io

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
	Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
	Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.

bernard@atmark.io

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Inquired of the Program Manager and determined that a standard production image was utilized for the installation and maintenance of each production server.	No deviations noted.
	Inspected a sample configuration of the tool Google uses to monitor the virtual machines and detection of deviations for the virtual machine.	No deviations noted.
	Inspected a sample of tickets and determined that deviations identified in virtual machines are detected and corrected.	No deviations noted.
12. Integrity checks are in place at the file system level to ensure data integrity.	Inquired of the Program Manager and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.
	Inspected the organization's security policies and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.
	Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations to ensure data integrity at the file system level.	No deviations noted.
	Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration to ensure data integrity at the file system level.	No deviations noted.

bernard@bottmake.io

Google Confidental Information

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Observed a Software Engineer insert a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
	Observed a Software Engineer modify a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
	Observed a Software Engineer delete a sample file in the directory of a haphazardly selected production machine and determined the tool detected the deleted sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.

bernardoquatrin@gmail.com

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
1. Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.	Inquired of the Operations Manager and determined critical power and telecommunications equipment in data centers were physically protected from disruption and damage.	No deviations noted.
	Observed a sample of data centers and determined that power and telecommunications equipment in data centers were physically protected from disruption and damage.	No deviations noted.
	Observed a sample of data centers and determined that temperature and humidity of data halls were within the configured thresholds.	No deviations noted.
2. Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).	Inquired of the Data Center Operations Manager and determined redundant power was utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power sources.	No deviations noted.
	Observed a sample of data centers and determined that network rooms were connected to an UPS system and emergency generator power was available for at least 24 hours in the event of a loss of power.	No deviations noted.
	Observed a sample of data centers and determined that data centers were equipped with redundant network connections via different physical connections.	No deviations noted.
	Inspected maintenance records for in-scope data centers and observed that equipment was continuously monitored and periodically tested.	No deviations noted.

bernie@bottmark.io

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
3. Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	Inquired of the Operations Manager and determined information systems and equipment were safeguarded against unauthorized entry and removal from data centers and data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	No deviations noted.
	Inspected internal documentation and determined that the organization maintains policies and guidelines around the security of storage devices during delivery and movement throughout the data center.	No deviations noted.
	Observed a sample of data centers and determined that Google had safeguards in place to protect information systems and equipment from unauthorized entry and removal from data centers.	No deviations noted.
	Observed a sample of data centers and determined that dedicated receiving and shipping areas were isolated from the main data center floor, network rooms and security systems.	No deviations noted.
	Inspected a sample of tickets created for data center equipment entering and exiting data centers and determined Google authorized, monitored, and controlled the shipments and maintained a record of the items.	No deviations noted.
4. The organization has policies and guidelines that govern how to keep the organization's physical	Inquired of the Data Center Security Manager and determined that he organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.	No deviations noted.

bernardsbottmayer.de

Google Confidental Information

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
workplaces, facilities, and property safe.	Inspected the organization's policies and guidelines and determined that physical protection guidelines were specified within each document.	No deviations noted.
5. The organization authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items.	Inquired of the Operations Manager and determined information systems and equipment were safeguarded against unauthorized entry and removal from data centers and data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	No deviations noted.
	Inspected internal documentation and determined that the organization maintains policies and guidelines around the security of storage devices during delivery and movement throughout the data center.	No deviations noted.
	Observed a sample of data centers and determined that that the organization had safeguards in place to protect information systems and equipment from unauthorized entry and removal from data centers.	No deviations noted.
	Observed a sample of data centers and determined that dedicated receiving and shipping areas were isolated from the main data center floor, network rooms and security systems.	No deviations noted.
	Inspected a sample of tickets created for data center equipment entering and exiting data centers and determined the organization authorized, monitored, and controlled the shipments and maintained a record of the items.	No deviations noted.

bernard@bathmate.io

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
6. Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.	Inquired of the Program Manager and determined user access to high-security areas in data centers was reviewed on a periodic basis and inappropriate access was removed in a timely manner.	No deviations noted.
	Inspected the internal policies and determined user access to high-security areas in data centers was reviewed on a periodic basis.	No deviations noted.
	Inspected a sample of data center access reviews and determined that reviews were performed completely and accurately in a timely manner by appropriate personnel.	No deviations noted.
	Inspected a sample of users marked as appropriate within a data center access review and determined the users were appropriate based on cost center and job title.	No deviations noted.
	Inspected a sample of inappropriate users identified as requiring removal within a data center access review and determined the users were removed in a timely manner.	No deviations noted.
7. Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.	Inquired of the Data Center Security Manager and determined visitors were required to gain approval from authorized personnel, have their identity verified and remain with an escort during the duration of their visit.	No deviations noted.
	Inspected the physical security policies and determined the organization required visitors to gain approval from authorized personnel, have their identity verified at the perimeter and remain with an escort during the duration of their visit.	No deviations noted.

bernardo@bankaki.io

Google Confidental Information

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Observed a sample of data centers and determined that individuals on-site had their identities verified before entering the data center floors.	No deviations noted.
	Inspected a sample of access requests to visit data centers and determined approvals were obtained from authorized personnel prior to the visits, and visitors remained with an escort during the duration of their visits.	No deviations noted.
8. Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Inquired of the Program Manager and determined security measures utilized in data centers were assessed periodically and the results were reviewed by executive management.	No deviations noted.
	Inspected a sample of the reviews performed and determined security measures utilized in all data centers were assessed periodically and the results were reviewed by executive management.	No deviations noted.
9. Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	Inquired of the Data Center Facilities Manager and determined that physical security measures were in place as described and are reviewed through the annual data center security review.	No deviations noted.
	Inspected a sample data center security review performed for the production facilities and determined that management reviewed the physical security measures at the facilities.	No deviations noted.
	Observed a sample of data centers and determined that visitors obtained approvals from authorized personnel prior to their visits, had their identities verified before entering the data center floors, and remained with an escort during the duration of their visits.	No deviations noted.

herron@hotmail.io

Google Confidental Information

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Observed a sample of data centers and determined that data centers were continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	No deviations noted.
	Observed a sample of data centers and determined that data centers were secured through the use of badge reader and biometric control systems.	No deviations noted.
	Inspected the badge reader activity logs for a sample of data centers and determined access to Google spaces was logged and monitored.	No deviations noted.
	Inspected the badge reader activity logs for a sample of data centers and determined logs were retained for at least 3 months.	No deviations noted.
10. Data center physical access logs are recorded and retained in accordance with organizational or regulatory requirements.	Inquired of the Data Center Facilities Manager and determined that physical security measures were in place as described and are reviewed through the annual data center security review.	No deviations noted.
	Inspected a sample data center security review performed for the production facilities and determined that management reviewed the physical security measures at the facilities.	No deviations noted.
	Observed a sample of data centers and determined that visitors obtained approvals from authorized personnel prior to their visits, had their identities verified before entering the data center floors, and remained with an escort during the duration of their visits.	No deviations noted.

bernard@batmaker.io

Google Confidental Information

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Observed a sample of data centers and determined that data centers were continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	No deviations noted.
	Observed a sample of data centers and determined that data centers were secured through the use of badge reader and biometric control systems.	No deviations noted.
	Inspected the badge reader activity logs for a sample of data centers and determined access to Google spaces was logged and monitored.	No deviations noted.
	Inspected the badge reader activity logs for a sample of data centers and determined logs were retained for at least 3 months.	No deviations noted.
11. Automated mechanisms are utilized to track inventory of all production machines and inventory of all serialized server components.	Inquired of the Data Center Operations Manager and determined automated mechanisms were utilized to track inventory of production machines.	No deviations noted.
	Inspected the records from the inventory system for a sample of production machines selected during data center inspections and determined the selected machines existed in the inventory system.	No deviations noted.
	Observed a sample of production machines selected from the inventory system prior to the data center inspection and determined that the selected machines existed at the data centers.	No deviations noted.

bernard@batmaker.io

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Inspected the relevant configuration and determined automated alerts were configured to track inventory of production machines.	No deviations noted.
	Inspected a sample of alerts generated when thresholds for the organization's inventory tracking processes were exceeded and determined alerts were appropriately generated, responded and resolved in a timely manner.	Deviation noted. For one (1) of twenty-five (25) sampled alert tickets generated to track inventory of production machines, we determined that the ticket was not resolved within the SLO guidelines for the assigned priority and severity.
	Inquired of management and determined if any control deviations were identified during their own internal testing procedures.	Per review of the first party audit report, for three (3) of twenty-five (25) sampled alert tickets generated to track inventory of production machines, we determined that the tickets were not resolved within the SLO guidelines for the assigned priority and severity.

bernard@botmaker.io

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Management's Response: Management acknowledges that four samples, one from EY's testing and three identified by first-party audit, were not resolved within our established internal Service Level Objectives (SLOs). For the sample found from EY's testing, management determined that this deviation was caused due to a delay within a planned dependent project. For three samples from first-party testing, management determined that these deviations were caused by dependent process delays. Throughout their lifecycle, the assets remained secure under multiple layers of physical security with appropriate supervision. These four tickets have since all been fully resolved, and we will continue to review the process of monitoring timely ticket resolution.	
12. Data centers are equipped with fire detection alarms and protection equipment.	Inquired of the Data Center Operations Facilities Manager and determined data centers were equipped with fire detection alarms and protection equipment.	No deviations noted.
	Observed a sample of data centers and determined that they were equipped with fire detection alarms and protection equipment.	No deviations noted.
	Observed a sample of data centers and determined that potential environmental threats to the data centers were anticipated and countermeasures were established based on the nature and geographical location of the data centers.	No deviations noted.

bernard@bottomline.io

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
1. Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Inquired of the Security Engineering Manager and determined audit logs were continuously monitored for events related to security, availability, processing integrity and confidentiality threats and alerts are generated for further investigation.	No deviations noted.
	Inspected internal documentation and determined there are guidelines used by the Security Surveillance Team to classify, prioritize, perform cause analysis, and triage the security incidents.	No deviations noted.
	Inspected internal documentation and determined the organization provides logging capabilities to its customers and customers can only access records related to their own activities.	No deviations noted.
	Observed a sample log configuration and determined log sources were monitored and maintained to continuously detect malicious or unusual insider activity.	No deviations noted.
	Observed a sample of alerts for events related to security, availability, processing integrity and confidentiality and determined alerts were generated when the pre-defined criteria was met.	No deviations noted.
	Observed the dashboard of monitoring tools and determined that alerts related to security, availability, processing integrity and confidentiality were monitored.	No deviations noted.
	Inspected that emergency changes are logged and subject to automated checks.	No deviations noted.

bernardo@otmdev.in

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inspected a sample of emergency changes that required manual investigation and determined whether they were appropriately resolved.	No deviations noted.
2. The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Inquired of the Program Manager and determined the organization had an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No deviations noted.
	Inspected the organization's incident response policy and determined policies and procedures were in place which outline a quick, effective, and orderly response to information security incidents. In addition, classification, prioritization, and escalation of security incidents per criticality are also identified and mechanisms are defined to measure and monitor the type and scope of security incidents.	No deviations noted.
	Inspected internal documentation and determined the organization maintained and periodically updated the incident response policy.	No deviations noted.
3. The organization maintains a framework that defines how to organize a response to security and privacy incidents.	Inquired of the Program Manager and determined the organization maintained a framework that defined how to organize a response to security and privacy incidents.	No deviations noted.
	Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.

bernardoholmer.io

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inspected relevant documentation and determined a process was in place for incident response teams to quantify, manage and monitor incidents.	No deviations noted.
4. Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inquired of the Program Manager and determined information security incidents were documented per the organization's Incident Response Policy. Information from these events could be used to prevent future incidents and as examples for information security training.	No deviations noted.
	Inspected the organization's incident response policies and determined it documented the process for reporting, responding to, and monitoring information security incidents.	No deviations noted.
	Inspected relevant internal documentation and determined information security trainings were implemented and that incidents were analyzed to prevent future incidents.	No deviations noted.
5. Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
	Inspected Google's security policies and determined Google had implemented rules to govern the installation of software by users.	No deviations noted.

bernardo@hotmail.com

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
	Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
	Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.

bernardo@tmb.or.id

Google Confidental Information

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inquired of the Program Manager and determined that a standard production image was utilized for the installation and maintenance of each production server.	No deviations noted.
	Inspected a sample configuration of the tool Google uses to monitor the virtual machines and detection of deviations for the virtual machine.	No deviations noted.
	Inspected a sample of tickets and determined that deviations identified in virtual machines are detected and corrected.	No deviations noted.
6. The organization has a dedicated team responsible for managing security and privacy incidents.	Inquired of the Program Manager and determined the organization had a dedicated team responsible for managing security and privacy incidents, and provides internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.
	Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.
	Inspected relevant documentation and determined the organization provided internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.

hernando@hotmail.io

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Observed the organization's incident management ticketing system and determined that mechanisms were in place to track internal and external reported security and privacy incidents through investigation and resolution.	No deviations noted.
7. The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inquired of the program manager and determined the organization provided monitoring tools to facilitate the detection and reporting of operational issues and the monitoring tools sent automated alerts to operational personnel based on predetermined criteria and are escalated per policy.	No deviations noted.
	Inspected relevant documentation and determined there were tools in place to detect and report operational issues to operational personnel.	No deviations noted.
	Inspected a sample of alerts and determined monitoring tools were in place to detect, report, escalate and resolve operational issues.	No deviations noted.
	Inspected evidence of escalated sample security incident and determined appropriate action was taken to identify, record, track and resolve the incident in a timely manner.	No deviations noted.
8. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Inquired of the program manager and determined the organization provided monitoring tools to facilitate the detection and reporting of operational issues and the monitoring tools sent automated alerts to operational personnel based on predetermined criteria and are escalated per policy.	No deviations noted.

bernard@bolmaker.in

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inspected relevant documentation and determined there were tools in place to detect and report operational issues to operational personnel.	No deviations noted.
	Inspected a sample of alerts and determined monitoring tools were in place to detect, report, escalate and resolve operational issues.	No deviations noted.
	Inspected evidence of escalated sample security incident and determined appropriate action was taken to identify, record, track and resolve the incident in a timely manner.	No deviations noted.
9. The organization provides internal personnel (employees and extended workforce) with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	Inquired of the Program Manager and determined the organization had a dedicated team responsible for managing security and privacy incidents, and provides internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.
	Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.
	Inspected relevant documentation and determined the organization provided internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.

hernando@bramaier.io

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Observed the organization's incident management ticketing system and determined that mechanisms were in place to track internal and external reported security and privacy incidents through investigation and resolution.	No deviations noted.
10. The organization provides external users with mechanisms to report security issues, incidents and concerns.	Inquired of the Program Manager and determined that the organization provides external users with mechanisms to report security issues, incidents, and concerns.	No deviations noted.
	Inspected the organization's websites and determined mechanisms were available for external users to report security issues, incidents, and concerns.	No deviations noted.
	Inspected the organization's websites and determined separate communication channels were in place to enable anonymous or confidential communication when normal channels were inoperative or ineffective.	No deviations noted.
	Inspected a sample incident ticket raised by an external user through the established mechanisms to validate that the issue or concern was received by the organization.	No deviations noted.
11. The organization has established a dedicated security team engaging in security and privacy of customer data and	Inquired of the Program Manager and determined that the organization has established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.	No deviations noted.

bernard@hotmaker.ro

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
managing security 24 x 7 worldwide.	Inspected relevant policies and guidelines and determined that the organization established a dedicated security team to engage in security and privacy of customer data.	No deviations noted.
	Inspected internal documentation and determined that a dedicated security team engaged in security and privacy of customer data managed security 24 x 7 worldwide.	No deviations noted.
	Inspected the on-call calendar configuration and determined that the on-call calendar was maintained according to a defined set of rules.	No deviations noted.
	Inspected the on-call calendar configuration and determined that on-call rotation schedules were automated and any change in the schedule was subject to the management's approval process.	No deviations noted.
	Inspected the Incident Response team's on-call schedule and determined that the security team engaged in security and privacy was available 24 x 7.	No deviations noted.

bernard@bitmaker.io

CO6 - Availability

Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.

Control Description	Tests Performed by EY	Results
1. Internal system clocks are synchronized to atomic clocks and GPS.	Inquired of the Program Manager and determined that internal system clocks were synchronized to atomic clocks and GPS.	No deviations noted.
	Inspected internal documentation and determined the organization established time synchronization service to a single reference time source.	No deviations noted.
	Inspected the relevant configurations and determined that internal system clocks were synchronized to atomic clocks and GPS.	No deviations noted.
	Inspected evidence showing the synchronization of internal system clocks to atomic clocks and GPS.	No deviations noted.
2. The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inquired of the Program Manager and determined the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	No deviations noted.
	Inspected a sample datastore configuration for a Google Cloud Platform product and determined the product was configured to replicate to support service redundancy, and availability.	No deviations noted.
	Inspected the Google Cloud Platform product's monitoring dashboard and determined resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy.	No deviations noted.

henry@bothpker.io

CO6 - Availability

Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.

Control Description	Tests Performed by EY	Results
	Inspected the Google Cloud Platform product's monitoring dashboard and determined resources were distributed across distinct, geographically dispersed processing facilities to support service availability.	No deviations noted.
3. The organization makes procedures related to the management of information processing resources available. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	Inquired of the Program Manager and determined the organization made available, procedures related to the management of information processing resources. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	No deviations noted.
	Inspected the organization's resource management documentation and determined an overview to monitor, maintain and evaluate storage and processing capacity demand had been provided.	No deviations noted.
	Inspected a sample monitoring dashboard and determined they are used to monitor and manage capacity of its information processing resources. Inspected a sample of automated notifications related to critical resource capacity utilization and determined alerts were appropriately set.	No deviations noted.
4. The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inquired the Program Manager and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
	Inspected the policies and documents related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.

bernardopotmajer.io

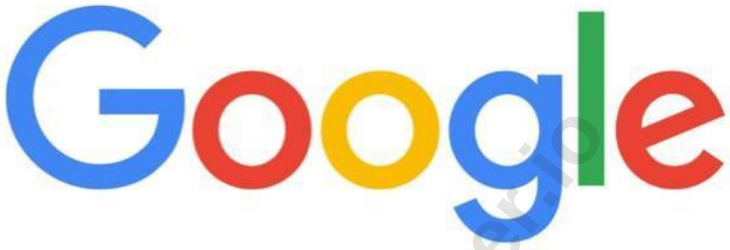
CO6 - Availability

Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.

Control Description	Tests Performed by EY	Results
	Inspected the configurations related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
5. The organization maintains business continuity plans to define how personnel should respond to disruptions.	Inquired of the Program Manager and determined the organization maintains business continuity plans to define how personnel should respond to disruptions.	No deviations noted.
	Inspected internal websites and determined that business continuity plans were maintained and made available to corresponding data center teams for organization-owned and third-party data centers.	No deviations noted.
	Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample of the Organization-owned data centers and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.
	Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample third-party data center and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.

bernd@bernaka.io

Google Confidental Information



System and Organization Controls (SOC) 2 Type II Report

Description of the Google Cloud Platform System

For the Period 01 August 2024 to 31 July 2025

With Independent Service Auditor's Report

Including Tests Performed and Results Thereof

bernard@botmaker.jp

Google Confidental Information

Table of Contents

SECTION I - Google's Management Assertion 1

SECTION II - Independent Service Auditor's Report 3

SECTION III - Description of the Google Cloud Platform System 8

A. Overview of Operations 9

B. Relevant Aspects of Internal Control 43

C. Policies 44

D. Communications 46

E. Procedures 47

F. Monitoring 59

G. User Entity Responsibilities 60

SECTION IV - Description of Criteria, Controls, Tests and Results of Tests 75

Testing performed and results of tests of entity level controls 76

Control criteria and related controls for systems and applications 76

Criteria, Controls, Tests and Results of Tests 77

Criteria to Controls Mapping 194

SECTION V - Other Information Provided by Google LLC 203

bernard@bormaker.io

SECTION I - Google's Management Assertion

bernard@botmaker.io

Google Confidental Information

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Google's Management Assertion

We have prepared the accompanying description titled "Description of the Google Cloud Platform System" (Description) of Google LLC ("Google" or "Service Organization") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Google Cloud Platform System (System) that may be useful when assessing the risks arising from interactions with the System, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA *Trust Services Criteria*.

We confirm, to the best of our knowledge and belief, that:

(a) The Description presents the System that was designed and implemented throughout the period 1 August 2024 to 31 July 2025 in accordance with the Description Criteria.
(b) The controls stated in the Description were suitably designed throughout the period 1 August 2024 to 31 July 2025 to provide reasonable assurance that Google's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period 1 August 2024 to 31 July 2025.
(c) The Google controls stated in the Description operated effectively throughout the period 1 August 2024 to 31 July 2025 to provide reasonable assurance that Google's service commitments and system requirements were achieved based on the applicable trust services criteria.

Google LLC
18 September 2025

bellard@hotmail.it

SECTION II - Independent Service Auditor's Report

bernard@botmaker.io

Google Confidental Information

Shape the future with confidence

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Independent Service Auditor's Report

To the Management of Google LLC:

Scope

We have examined Google LLC's (referred to hereafter as "Google" or "the Company") accompanying description titled "Description of the Google Cloud Platform System" of its Google Cloud Platform system for the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and provided to user entities throughout the period 1 August 2024 to 31 July 2025 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period 1 August 2024 to 31 July 2025 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA Trust Services Criteria.

The information in the accompanying "SECTION V - Other Information Provided by Google LLC" is presented by management of Google to provide additional information and is not part of Google's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly, we express no opinion on it.

Google's responsibilities

Google is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that its service commitments and system requirements were achieved. Google has provided the accompanying assertion titled, "Google's Management Assertion" (Assertion), about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Google is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

bernard@bountin.io

Google Confidental Information

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls stated therein to achieve the service organization's service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period 1 August 2024 to 31 July 2025. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of those controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria
- Evaluating the overall presentation of the Description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Our examination was not conducted for the purpose of evaluating the performance or integrity of Google's AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of Google's AI services.

We are required to be independent of Google and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the *Preface: Applicable to All Members* and *Part*

bernard@botmaker.io

Google Confidental Information

1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA. We have complied with such independence and other ethical requirements and applied the AICPA's Statements on Quality Control Standards.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the service commitments and system requirements based on the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying "SECTION IV - Description of Criteria, Controls, Tests and Results of Tests" (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

(a) The Description presents the Google Cloud Platform System that was designed and implemented throughout the period 1 August 2024 to 31 July 2025 in accordance with the Description Criteria.
(b) The controls stated in the Description were suitably designed throughout the period 1 August 2024 to 31 July 2025 to provide reasonable assurance that Google's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period.
(c) The controls stated in the Description operated effectively throughout the period 1 August 2024 to 31 July 2025 to provide reasonable assurance that Google's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Google, user entities of the Google Cloud Platform System during some or all of the period 1 August 2024 to 31 July 2025 and prospective user

bernard@bdmarden.no

Google Confidental Information

Shape the future with confidence

entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

18 September 2025
San Jose, CA

bernard@botmaker.io

SECTION III - Description of the Google Cloud Platform System

bernard@botmaker.io

Google Confidental Information

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Description of the Google Cloud Platform System

A. Overview of Operations

Google LLC (“Google” or “the Company”), an Alphabet subsidiary, is a global technology service provider focused on improving the ways people connect with information. Google’s innovations in web search and advertising have made Google’s website one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world’s largest online index of websites and other content, and makes this information freely available to anyone with an Internet connection. Google’s automated search technology helps people obtain nearly instant access to relevant information from their vast online index.

Google Cloud Platform provides Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) and, allowing businesses and developers to build and run any or all of their applications on Google’s Cloud infrastructure. Customers can benefit from the performance, scale, reliability, ease-of-use, and a pay-as-you-go cost model.

Google’s product offerings for Google Cloud Platform (GCP) provide the unique advantage of leveraging the resources of Google’s core engineering team while also having a dedicated team to develop solutions for the corporate market. As a result, these Google offerings are positioned to innovate at a rapid rate and provide the same level of service that users are familiar with on google.com.

This report only applies to the underlying infrastructure and systems that support the services outlined below. The examination was also not conducted for the purpose of evaluating the performance or integrity of Google’s AI services or models.

Google Cloud Platform includes the following services, hereafter described collectively as “Google Cloud Platform” or "GCP":

- Artificial Intelligence (AI) and Machine Learning (ML) - Innovative, scalable machine learning services, with pre-trained models and the ability to generate tailored models
- Application Programming Interface (API) Management - Develop, deploy, and manage APIs on any Google Cloud back end
- Compute - A range of computing options tailored to match the size and needs of any organization
- Data Analytics - Tools to capture, process, store and analyze data on a single platform
- Databases - Migrate, manage, and modernize data with secure, reliable, and highly available relational and nonrelational databases

Google

- Developer Tools - A collection of tools and libraries that help development teams work more quickly and effectively
- Healthcare and Life Sciences - Healthcare solution to protect sensitive data and maintain compliance with numerous requirements across various domains, geographies, and workloads
- Hybrid and Multi-cloud - Connect on-premises or existing cloud infrastructure with Google Cloud's scalability and innovation
- Management Tools - Manage apps on GCP with a web-based console, mobile app, or Cloud Shell for real time monitoring, logging, diagnostics, and configuration
- Media and Gaming - Build user experiences and empower developers by minimizing infrastructure complexity and accelerating data insights
- Migration - Large-scale, secure online data transfers to Cloud Storage and databases
- Networking - A private network using software-defined networking and distributed systems technologies to host and deliver services around the world
- Operations - Suite of products to monitor, troubleshoot, and improve application performance on Google Cloud environments
- Security and Identity - Manage the security and access to cloud assets, supported by Google's own protection of its infrastructure
- Serverless Computing - Deploy functions or apps as source code or as containers without worrying about the underlying infrastructure. Build full stack serverless applications with Google Cloud's storage, databases, machine learning, and more
- Storage - Scalable storage options and varieties for different needs and price points
- Other - Additional GCP services supporting e-commerce, procurement, billing, and petabyte-scale scientific analysis and visualization of geospatial datasets

The Google Cloud Platform products covered in this system description consist of the following services:

- Artificial Intelligence (AI) and Machine Learning (ML)
- Agent Assist
- Agentspace[5]
- AI Platform Deep Learning Container
- AI Platform Training and Prediction[3]
- Anti-Money Laundering (AML) AI
- AutoML Tables
- AutoML Translation
- Cloud Natural Language API
- Cloud Speaker ID
- Cloud Translation
- Cloud Vision
- Conversational AI (formerly Contact Center AI (CCAI)

bernard@bonnaker.io

Google Confidental Information

Google

- Conversational Insights (formerly Contact Center AI Insights)
- Dialogflow
- Document AI
- Document AI Warehouse
- Food Ordering AI Agent
- Gemini Code Assist[5]
- Gemini for Google Cloud
- Gemini in BigQuery[5]
- Generative AI on Vertex AI
- Google Cloud Contact Center as a Service (CCaaS)
- NotebookLM for Enterprise[5]
- Ray on Vertex AI
- Recommendations AI
- Retail Search
- Speech-to-Text
- Talent Solution
- Text-to-Speech
- Vertex AI Codey[4]
- Vertex AI Colab Enterprise
- Vertex AI Conversation
- Vertex AI Platform
- Vertex AI Search
- Vertex AI Workbench Instances
- Video Intelligence API

- Application Programming Interface (API) Management
  - Advanced API Security
  - Apigee
  - API Gateway
  - Application Integration
  - Cloud Endpoints
  - Integration Connectors

- Compute
  - App Engine
  - Batch
  - Compute Engine
  - Workload Manager

bernard@botmaker.io

Google Confidental Information

Google

- Data Analytics
  - BigQuery
  - Cloud Composer
  - Cloud Data Fusion
  - Cloud Life Sciences
  - Data Catalog
  - Dataflow
  - Dataform
  - Dataplex
  - Dataproc
  - Dataproc Metastore
  - Looker (Google Cloud core)
  - Looker Studio
  - Managed Service for Apache Kafka[1]
  - Pub/Sub
- Databases
  - AlloyDB
  - Cloud Bigtable
  - Cloud Spanner
  - Cloud SQL
  - Datastore
  - Firestore
  - Memorystore
- Developer Tools
  - Artifact Analysis
  - Artifact Registry
  - Cloud Build
  - Cloud Source Repositories
  - Cloud Workstations
  - Container Registry
  - Firebase Test Lab
  - Google Cloud Deploy
  - Google Cloud SDK
  - Infrastructure Manager
  - Secure Source Manager
- Healthcare and Life Sciences

bernard@botmaker.io

Google

  - Cloud Healthcare
  - Healthcare Data Engine (HDE)
- Hybrid and Multi-cloud
  - Connect
  - Google Kubernetes Engine
  - GKE Enterprise Config Management
  - GKE Identity Service
  - Hub
  - Knative serving
  - Service Mesh
- Management Tools
  - Cloud Console
  - Cloud Console App
  - Cloud Deployment Manager
  - Cloud Shell
  - Recommender
  - Service Infrastructure
- Media and Gaming
  - Media CDN
  - Transcoder API
- Migration
  - BigQuery Data Transfer Service
  - Database Migration Service
  - Migration Center
  - Migrate to Virtual Machines
  - Storage Transfer Service
- Networking
  - Cloud CDN
  - Cloud DNS
  - Cloud IDS (Cloud Intrusion Detection System)
  - Cloud Interconnect
  - Cloud Load Balancing
  - Cloud Network Address Translation (NAT)
  - Cloud NGFW

bernard@botmaker.io

Google

- Cloud Router
- Cloud Service Mesh
- Cloud Virtual Private Network (VPN)
- Google Cloud Armor
- Network Connectivity Center
- Network Intelligence Center
- Network Service Tiers
- Service Directory
- Spectrum Access System
- Traffic Director
- Virtual Private Cloud (VPC)

- Operations
  - Cloud Logging
  - Cloud Monitoring
  - Cloud Profiler
  - Cloud Trace
  - Google Cloud Backup and DR
  - Personalized Service Health

- Security and Identity
  - Access Approval
  - Access Context Manager
  - Access Transparency
  - Assured Workloads
  - Binary Authorization
  - Certificate Authority Service
  - Certificate Manager
  - Chrome Enterprise Premium
  - Cloud Asset Inventory
  - Cloud External Key Manager (Cloud EKM)
  - Cloud Hardware Security Module (HSM)
  - Cloud Key Management Service (KMS)
  - Firebase App Check
  - Firebase Authentication
  - Google Cloud Identity-Aware Proxy
  - Google Threat Intelligence[2]
  - Google Security Operations (SIEM)[2]
  - Google Security Operations (SOAR)[2]

bernard@botmaker.io

Google Confidental Information

Google

  - GTI for Google Security Operations[2]
  - Identity & Access Management (IAM)
  - Identity Platform
  - Key Access Justifications (KAJ)
  - Managed Service for Microsoft Active Directory (AD)
  - Organization Policy[1]
  - Privileged Access Manager
  - reCAPTCHA Enterprise
  - Resource Manager API
  - Risk Manager
  - SecLM
  - Secret Manager
  - Security Command Center
  - Sensitive Data Protection (including Cloud Data Loss Prevention)
  - VirusTotal
  - VPC Service Controls
  - Web Risk API
- Serverless Computing
  - Cloud Functions
  - Cloud Functions for Firebase
  - Cloud Run
  - Cloud Scheduler
  - Cloud Tasks
  - Datastream
  - Eventarc
  - Workflows
- Storage
  - Backup for GKE
  - Cloud Filestore
  - Cloud Storage
  - Cloud Storage for Firebase
  - Parallelstore[1]
  - Persistent Disk
- Other
  - Cloud Billing
  - Google Earth Engine

bernard@botmaker.io

- Google Cloud Marketplace
- Google Cloud Skills Boost[1]
- Tables

[1] Indicates products in scope only for the period 1 March 2025 through 31 July 2025

[2] Google Security Operations (SIEM), Google Security Operations (SOAR) and Google Threat Intelligence (GTI) for Google Security Operations are covered by separate terms than GCP. Refer to the Terms of Services (https://cloud.google.com/terms/secops/service-terms) for additional details

[3]The AI Platform Training & Prediction product was deprecated on January 31, 2025.

[4]The Vertex AI Codey product was deprecated on April 21, 2025.

[5] Indicates products in scope only for the period 1 May 2025 through 31 July 2025

The products are composed of communication, productivity, collaboration, and security tools that can be accessed from virtually any location with secure Internet connectivity. This means every employee and each user entity they work with can be productive from anywhere, using any device with a secure Internet connection.

These products provide a comprehensive variety of technical services that organizations rely on:

Artificial Intelligence (AI) and Machine Learning (ML)

Google does not use Customer Data to train or fine-tune any AI/ML models without a customer's prior permission or instruction. Refer to the service terms (https://cloud.google.com/terms/service-terms) for additional details.

Agent Assist

Agent Assist is a Large Language Model (LLM)- powered AI solution that increases human agent productivity and enhances customer service by offering real-time assistance.

Agentspace

Agentspace combines AI Agents, Gemini models, and Google search technologies to enable automation and enhance employee productivity by connecting enterprise data sources and applications, offering workflow automation, search functionality, and generative AI features.

AI Platform Deep Learning Container

AI Platform Deep Learning Container provides Docker images with AI frameworks that can be customized and used with Google Kubernetes Engine (GKE), Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.

bernard@botmaker.io

AI Platform Training and Prediction

AI Platform Training and Prediction is a managed service that enables users to easily build machine learning models with popular frameworks like TensorFlow, XGBoost and Scikit Learn. It provides scalable training and prediction services that work on large datasets.

Anti-Money Laundering (AML) AI

AML AI is a machine learning engine which takes customer data and training labels to create a tailored model covering an extensible typology of risks for AML along with governance documentation to ease adoption in this highly regulated environment.

AutoML Tables

AutoML Tables enables data scientists, analysts, and developers to automatically build and deploy machine learning models on structured data at increased speed and scale.

AutoML Translation

AutoML Translation is a simple and scalable translation solution that allows businesses and developers with limited machine learning expertise to customize the Google Neural Machine Translation (GNMT) model for their own domain or use-case.

Cloud Natural Language API

Cloud Natural Language API provides natural language understanding as a simple to use Application Programming Interface (API). Given a block of text, this API enables finding entities, analyzing sentiment (positive or negative), analyzing syntax (including parts of speech and dependency trees), and categorizing the content into a rich taxonomy. The API can be called by passing the content directly or by referring to a document in Cloud Storage.

Cloud Speaker ID

Speaker ID allows customers to enroll user voice prints and later verify users against a previously enrolled voice print.

Cloud Translation

Cloud Translation automatically translates text from one language to another language (e.g., French to English). The API is used to programmatically translate text in webpages or apps.

Cloud Vision

Cloud Vision enables the understanding of image content by encapsulating machine learning models in a Representational State Transfer (REST) API. It classifies images into thousands of categories, detects individual objects and faces within images, and finds and reads printed words contained within images. It can be applied to build metadata on image catalogs, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. It can also analyze images uploaded in the request and integrate with image storage on Google Cloud Storage.

bernardo@botmaker.io

Google Confidental Information

Conversational AI (formerly Contact Center AI (CCAI)

Conversational AI uses AI to improve the customer experience in contact centers. It includes Agent Assist, Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Insights, Speech-to-Text, Text-to-Speech, and Speaker ID.

Conversational Insights (formerly Contact Center AI Insights)

Conversational Insights helps customers extract value from their contact center data by identifying sentiment and topics and highlighting key insights in the data.

Dialogflow

Dialogflow is a development suite for voice and text conversational apps including chatbots. Dialogflow is cross-platform and can connect to apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Actions on Google, Facebook Messenger, Slack).

Document AI

Document AI classifies and extracts structured data from documents to help streamline data validation and automate business processes.

Document AI Warehouse

Document AI Warehouse is a data management and governance platform that stores, searches, and organizes documents and their extracted and tagged metadata. Document AI Warehouse is highly scalable and fully managed and can be integrated with enterprise document workflows, applications, and repositories.

Food Ordering AI Agent

A repeatable, scalable Food Ordering Voice Assistant that helps restaurants serve their customers with high quality and consistent service.

Google Cloud Contact Center as a Service (CCaaS)

Google Cloud CCaaS is a contact-center-as-a-service (CCaaS) platform leveraging Conversational AI. It integrates directly with CRMs and queues and routes customer interactions across voice and digital channels to resource pools, including human agents.

Gemini Code Assist

Gemini Code Assist provides AI-powered assistance to help customer development teams build, deploy, and operate applications throughout the software development lifecycle.

Gemini for Google Cloud

Gemini for Google Cloud provides AI-powered end user assistance with a wide range of Google Cloud products. Gemini for Google Cloud is a generative AI-powered collaboration Service that provides assistance to Google Cloud end users. Gemini for Google Cloud is embedded in many

bernard@botmaker.io

Google Cloud products to provide developers, data scientists, and operators an integrated assistance experience.

Gemini in BigQuery

Gemini in BigQuery provides AI-powered assistance to help customers understand, query, and work with their data across the entire data lifecycle.

Generative AI on Vertex AI

Generative AI on Vertex AI includes features for generative AI use cases, including large language, text-to-image, and image-to-text models.

NotebookLM for Enterprise

NotebookLM for enterprise enables customers to use generative AI to summarize and extract information from their data.

Ray on Vertex AI

Ray on Vertex AI is an open-source framework for scaling AI and Python applications. Ray provides the infrastructure to perform distributed computing and parallel processing for the user's machine learning (ML) workflow.

Recommendations AI

Recommendations AI enables customers to build a personalized recommendation system using ML models.

Retail Search

Retail Search allows retailers to leverage Google's search capabilities on their retail websites and applications.

Speech-to-Text

Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy-to-use API.

Talent Solution

Talent Solution offers access to Google's machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.

Text-to-Speech

Text-to-Speech synthesizes human-like speech based on input text in a variety of voices and languages.

bernard@botmaker.io

Vertex AI Codey

Vertex AI Codey is a suite of models that work with code that includes the following APIs:

- The code generation API - Generates code based on a natural language description of the desired code.
- The code chat API - Can power a chatbot that assists with code-related questions.
- The code completion API - Provides code autocompletion suggestions as users write code.

Vertex AI Colab Enterprise

Vertex AI Colab Enterprise is a collaborative, managed notebook environment with the security and compliance capabilities of Google Cloud.

Vertex AI Conversation

Vertex AI Conversation allows customers to leverage foundational models and conversational AI to create multimodal chat or voice agents.

Vertex AI Platform

Vertex AI Platform is a service for managing the AI and machine learning development lifecycle. Customers can (i) store and manage datasets, labels, features, and models; (ii) build pipelines to train and evaluate models and run experiments using Google Cloud algorithms or custom training code; (iii) deploy models for online or batch use cases; (iv) manage data science workflows using Colab Enterprise and Vertex AI Workbench (also known as Notebooks); and (v) create business optimization plans with Vertex Decision Optimization.

Vertex AI Search

Vertex AI Search allows customers to leverage foundational models and search and recommendation technologies to create multimodal semantic search and question-answering experiences.

Vertex AI Workbench Instances

Vertex AI Workbench instances are Jupyter notebook-based development environments for the entire data science workflow. Users can interact with Vertex AI and other Google Cloud services from within a Vertex AI Workbench instance's Jupyter notebook.

Video Intelligence API

Video Intelligence API makes videos searchable, and discoverable, by extracting metadata through a REST API. It annotates videos stored in Google Cloud Storage and helps identify key noun entities in a video and when they occur within the video.

bernard@ohtmaker.io

Google

API Management

Advanced API Security

Advanced API Security acts as the users' API's vigilant guardian. It constantly analyzes incoming traffic, seeking out anomalous patterns that might indicate attacks or abuse. When suspicious activity is spotted, it can block harmful requests or alert users for further action. Additionally, it evaluates the users' API setups against security best practices, offering recommendations for improvement. This comprehensive approach helps users proactively safeguard the users' APIs, protect sensitive data, and ensure the users' API configurations are designed to withstand security challenges.

Apigee

Apigee is a full-lifecycle API management platform that lets customers design, secure, analyze, and scale APIs, giving them visibility and control. Apigee is available as Apigee, a fully managed service, Apigee hybrid, a hybrid model that's partially hosted and managed by the customer, or Apigee Private Cloud, an entirely customer hosted Premium Software solution. Apigee Private Cloud is not in scope for this report.

API Gateway

API Gateway is a fully managed service that enables users to develop, deploy, and secure APIs running on Google Cloud Platform.

Application Integration

Application Integration is an Integration-Platform-as-a-Service (iPaaS) that offers a comprehensive set of integration tools to connect and manage the multitude of applications and data required to support various business operations. Application Integration provides a unified drag and drop integration designer interface, triggers that help invoke an integration, configurable tasks and numerous connectors that allow connectivity to business applications, technologies, and other data sources using the native protocols of each target application.

Cloud Endpoints

Cloud Endpoints is a tool that provides services to develop, deploy, secure and monitor APIs running on Google Cloud Platform.

Integration Connectors

Integration Connectors is a platform that allows customers to connect to business applications, technologies and other data sources using native protocols of each target application. The connectivity established through these connectors helps manage access to various data sources which can be used with other services like Application Integration through a consistent, standard interface.

renard@botmaker.io

Google Confidental Information

Compute

App Engine

App Engine enables the building and hosting of web apps on the same systems that power Google applications. App Engine offers fast development and deployment of applications without the need to manage servers or other low-level infrastructure components. Scaling and software patching are handled by App Engine on the user's behalf. App Engine also provides the ability to create managed virtual machines (VMs). In addition, client APIs can be built for App Engine applications using Google Cloud Endpoints.

Batch

Batch is a fully managed service that lets users schedule, queue, and execute batch processing workloads on Compute Engine virtual machine (VM) instances. Batch provisions resources and manages capacity on users' behalf, allowing user batch workloads to run at scale.

Compute Engine

Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud. With virtual machines that can boot in minutes, it offers many configurations including custom machine types that can be optimized for specific use cases as well as support for Graphics Processing Units (GPUs), Tensor Processing Units (TPUs) and Local Solid-State Drive (SSD). Additionally, customers can enable Shielded VMs to provide advanced platform security.

Workload Manager

Workload Manager is a rule-based validation service for evaluating workloads running on Google Cloud. If enabled, Workload Manager scans application workloads to detect deviations from standards, rules, and best practices that improve system quality, reliability, and performance.

Data Analytics

BigQuery

BigQuery is a fully managed, petabyte-scale analytics data warehouse that features scalable data storage and the ability to perform ad hoc queries on multi-terabyte datasets. BigQuery allows users to share data insights via the web and control access to data based on business needs.

Cloud Composer

Cloud Composer is a managed workflow orchestration service that can be used to author, schedule, and monitor pipelines that span across clouds and on-premises data centers.

Cloud Data Fusion

Cloud Data Fusion is a fully managed, cloud native, enterprise data integration service for building and managing data pipelines. Cloud Data Fusion provides a graphical interface that allows customers to build scalable data integration solutions to cleanse, prepare, blend, transfer, and transform data.

bernard@notmaker.io

Google Confidental Information

Google

Cloud Life Sciences

Cloud Life Sciences is a suite of services and tools to store, process, inspect and share biomedical data, DNA sequence reads, reference-based alignments, and variant calls, using Google's cloud infrastructure.

Data Catalog

Data Catalog is a fully managed and scalable metadata management service that allows organizations to have a centralized and unified view of data assets.

Dataflow

Dataflow is a fully managed service for consistent, parallel data-processing pipelines. It utilizes the Apache Beam Software Development Kits (SDKs) with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the lifecycle of Compute Engine resources for the processing pipeline(s) and provides a monitoring interface for understanding pipeline health.

Dataform

Dataform is a service for data analysts to develop, test, version control, and schedule complex SQL workflows for data transformation in BigQuery. Dataform lets users manage data transformation in the Extraction, Loading, and Transformation (ELT) process for data integration. After raw data is extracted from source systems and loaded into BigQuery, Dataform helps users to transform it into a well-defined, tested, and documented suite of data tables.

Dataplex

Dataplex is an intelligent data fabric that helps customers unify distributed data and automate management and governance across that data to power analytics at scale.

Dataproc

Dataproc is a managed service for distributed data processing. It provides management, integration, and development tools for deploying and using Apache Hadoop, Apache Spark, and other related open source data processing tools. With Cloud Dataproc, clusters can be created and deleted on-demand and sized to fit whatever workload is at hand.

Dataproc Metastore

Dataproc Metastore provides a fully-managed metastore service that simplifies technical metadata management and is based on a fully-featured Apache Hive metastore. Dataproc Metastore can be used as a metadata storage service component for data lakes built on open source processing frameworks like Apache Hadoop, Apache Spark, Apache Hive, Presto, and others.

bernard@bomakers.io

Google Confidental Information

Google

Looker (Google Cloud core)

Looker (Google Cloud core) is a business intelligence and embedded analytics solution hosted on Google infrastructure. With Looker (Google Cloud core), customers can build semantic models using various data sources, develop customized insights from the models, and share those insights for collaboration via dashboards and other services.

Looker Studio

Looker Studio is a visualization and business intelligence product that enables users to connect to multiple datasets and turn their data into informative, easy to share, and fully customizable dashboards and reports.

Managed Service for Apache Kafka

Managed Service for Apache Kafka is a Google Cloud service that helps you run secure, scalable open source Apache Kafka clusters.

Pub/Sub

Pub/Sub provides reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a topic while other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Cloud Pub/Sub allows communication between independent applications.

Databases

AlloyDB

AlloyDB is an enterprise grade database product that combines the familiarity of open source DB front-ends, like PostgreSQL, with custom-built storage, query and connectivity layers for superior availability, performance, security and manageability.

Cloud Bigtable

Cloud Bigtable is a low-latency, fully managed, highly scalable NoSQL database service. It is designed for the retention and serving of data from gigabytes to petabytes in size.

Cloud Spanner

Cloud Spanner is a fully managed, scalable, relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and ACID (Atomicity, Consistency, Isolation, Durability) transactions with synchronous replication of data across regions.

Cloud SQL

Cloud SQL is a service to create, configure, and use managed third-party relational databases in Google Cloud Platform. Cloud SQL maintains, manages, and administers those databases.

bernard@bolmaker.io

Google Confidental Information

Google

Datastore

Datastore is a highly scalable NoSQL database for mobile and web applications. It provides query capabilities, atomic transitions, index, and automatically scales up and down in response to load.

Firestore

Firestore is a fully managed, scalable, serverless NoSQL document database for mobile, web, and server development. It provides query capabilities, live synchronization, and offline support.

Memorystore

Memorystore for Redis (Remote Dictionary Server) provides a fully managed in-memory data store service for GCP. Cloud Memorystore can be used to build application caches that provide low latency data access. Cloud Memorystore is compatible with the Redis protocol, allowing seamless migration with no code changes.

Developer Tools

Artifact Analysis

Artifact Analysis is a family of services that provide software composition analysis, metadata storage and retrieval. Its detection points are built into a number of Google Cloud products such as Artifact Registry and Google Kubernetes Engine (GKE) for quick enablement. The service works with both Google Cloud's first-party products and also lets users store information from third-party sources. The scanning services leverage a common vulnerability store for matching files against known vulnerabilities.

Artifact Registry

Artifact Registry is a service for managing container images and packages. It is integrated with Google Cloud tooling and runtimes and comes with support for native artifact protocols. This makes it simple to integrate it with user CI/CD tooling to set up automated pipelines.

Cloud Build

Cloud Build allows for the creation of container images from application source code located in Cloud Storage or in a third-party service (e.g., Github, Bitbucket). Created container images can be stored in Container Registry and deployed on Container Engine, Compute Engine, App Engine Flexible Environment, or other services to run applications from Docker containers.

Cloud Source Repositories

Cloud Source Repositories provides Git version control to support collaborative development of any application or service as well as a source browser that can be used to browse the contents of repositories and view individual files from within the Cloud Console. Cloud Source Repositories and related tools (e.g., Cloud Debugger) can be used to view debugging information alongside code during application runtime.

bernard@hotmaker.ro

Google Confidental Information

Google

Cloud Workstations

Cloud Workstations provides preconfigured, customizable, and secure managed development environments on Google Cloud. Cloud Workstations is accessible through a browser-based Integrated Development Environment (IDE), from multiple local code editors (such as IntelliJ IDEA Ultimate or VS Code), or through SSH. Instead of manually setting up development environments, users can create a workstation configuration specifying user environments in a reproducible way.

Container Registry

Container Registry is a private Docker image storage system on Google Cloud Platform.

Firebase Test Lab

Firebase Test Lab provides cloud-based infrastructure for testing apps on physical and virtual devices. Developers can test their apps across a wide variety of devices with Firebase Test Lab.

Google Cloud Deploy

Google Cloud Deploy is a managed service that automates delivery of user applications to a series of target environments in a defined promotion sequence. When users want to deploy updated applications, users create a release, whose lifecycle is managed by a delivery pipeline.

Google Cloud SDK

Google Cloud SDK is a set of tools to manage resources and applications hosted on Google Cloud Platform. It includes the Google Cloud Command Line Interface (CLI), Cloud Client Libraries for programmatic access to Google Cloud Platform services, the gsutil, kubectl, and bq command line tools, and various service and data emulators for local platform development. The Google Cloud SDK provides the primary programmatic interfaces to Google Cloud Platform.

Infrastructure Manager

Infrastructure Manager is a managed service that automates the deployment and management of Google Cloud infrastructure resources. Infrastructure is defined using Terraform and deployed onto Google Cloud by Infra Manager, enabling users to manage resources using Infrastructure as Code (IaC).

Secure Source Manager

Secure Source Manager is a fully-managed service that provides a Git-based source code management system.

Healthcare and Life Sciences

Cloud Healthcare

Cloud Healthcare provides managed services and an API to store, process, manage, and retrieve healthcare data in a variety of industry standard formats.

bernard@botmaker.io

Google Confidental Information

Healthcare Data Engine (HDE)

HDE is a solution that enables (1) harmonization of healthcare data to the Fast Healthcare Interoperability Resources (“FHIR”) standard and (2) streaming of healthcare data to an analytic environment.

Hybrid and Multi-cloud

The scope of the services included in this report is limited to the services managed by Google and does not extend to the application of the services in other cloud service providers' environments by the user entity. Refer to the Terms of Services (https://cloud.google.com/terms/services) for additional details.

Connect

Connect is a service that allows users to connect Kubernetes clusters to Cloud. This enables both users and Google-hosted components to interact with clusters through a connection to the in-cluster Connect software agent.

Google Kubernetes Engine

Google Kubernetes Engine, powered by the open source container scheduler Kubernetes, runs containers on Google Cloud Platform. Kubernetes Engine manages provisioning and maintaining the underlying virtual machine cluster, scaling applications, and operational logistics such as logging, monitoring, and cluster health management.

GKE Enterprise Config Management

GKE Enterprise Config Management is a policy management solution for enabling consistent configuration across multiple Kubernetes clusters. GKE Enterprise Config Management allows customers to specify one single source of truth and then enforce those policies on the clusters.

GKE Identity Service

GKE Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple environments. Users can log in to and access their clusters from the command line or from the Cloud Console, all using their existing identity providers.

Hub

Hub is a centralized control-plane that enables a user to centrally manage features and services on customer-registered clusters running in a variety of environments, including Google’s cloud, on-premises in customer data centers, or other third-party clouds.

Knative serving

Knative serving is Google's managed and fully supported Knative offering. Knative serving abstracts away the complexity of Kubernetes, making it easy to build and deploy user’s serverless workloads across hybrid and multi-cloud environments.

bernard@bolmaker.io

Google Confidental Information

Google

Service Mesh

Service Mesh is a managed service mesh service that includes (i) a managed certificate authority that issues cryptographic certificates that identify customer workloads within the Service Mesh for mutual authentication, and (ii) telemetry for customers to manage and monitor their services. Customers receive details showing an inventory of services, can understand their service dependencies, and receive metrics for monitoring their services. Service Mesh is provided as a service and as a software. The Service Mesh software offering is not in scope for this report.

Management Tools

Cloud Console

Cloud Console is a web-based interface used to build, modify, and manage services and resources on the Google Cloud Platform. Cloud services can be procured, configured, and run from Cloud Console.

Cloud Console App

Cloud Console App is a native mobile app that provides monitoring, alerting, and the ability to take actions on resources.

Cloud Deployment Manager

Cloud Deployment Manager is an infrastructure management service which automates creation, and management of Google Cloud Platform resources.

Cloud Shell

Cloud Shell provides command-line access to Google Cloud Platform resources through an in-browser Linux shell backed by a temporary Linux VM in the cloud. It allows projects and resources to be managed without having to install additional tools on systems and comes equipped and configured with common developer tools such as text editors, a MySQL client and Kubernetes.

Recommender

Recommender automatically analyzes usage patterns to provide recommendations and insights across services to help use Google Cloud Platform in a more secure, cost-effective, and efficient manner.

Service Infrastructure

Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services. It includes:

- Service Management API, which lets service producers manage their APIs and services;
- Service Consumer Management API, which lets service producers manage their relationships with their service consumers;
- Service Control API, which lets managed services integrate with Service Infrastructure for admission control and telemetry reporting functionality; and

bernard@hotmaker.it

- Service Usage API, which lets service consumers manage their usage of APIs and services

Media and Gaming

Media CDN

Media CDN is a planet-scale content delivery network allowing customers to automate all facets of deployment and management. Stream media and deliver exceptional experiences to customer end users, no matter where they are.

Transcoder API

Transcoder API can batch convert media files into optimized formats to enable streaming across web, mobile, and living room devices. It provides fast, easy to use, large-scale processing of advanced codecs while utilizing Google's storage, networking, and delivery infrastructure.

Migration

BigQuery Data Transfer Service

BigQuery Data Transfer Service automates data movement from Software as a Service (SaaS) applications to BigQuery on a scheduled, managed basis.

Database Migration Service

Database Migration Service is a fully managed migration service that enables users to perform high fidelity, minimal-downtime migrations at scale. Users can use Database Migration Service to migrate from on-premises environments, Compute Engine, and other clouds to certain Google Cloud-managed databases.

Migration Center

Migration Center provides tools, best practices and data-driven prescriptive guidance designed to accelerate the end-to-end cloud migration journey through business case development, environment discovery, workload mapping, migration planning, financial analysis, foundation setup and migration execution.

Migrate to Virtual Machines

Migrate to Virtual Machines is a fully-managed migration service that enables customers to migrate workloads at scale into Google Cloud Compute Engine with minimal down time by utilizing replication-based migration technology.

Storage Transfer Service

Storage Transfer Service provides the ability to import large amounts of online data into Google Cloud Storage. It can transfer data from Amazon Simple Storage Service (Amazon S3) and other HTTP/HTTPS locations as well as transfer data between Google Cloud Storage buckets.

bernard@botmaker.ro

Google

Networking

Cloud CDN

Cloud Content Delivery Network (CDN) uses Google's distributed network edge points of presence to cache HTTP(S) load balanced content.

Cloud DNS

Cloud DNS is a fully managed Domain Name System (DNS) service which operates a geographically diverse network of high-availability authoritative name servers. Cloud DNS provides a service to publish and manage DNS records for applications and services.

Cloud IDS (Cloud Intrusion Detection System)

Cloud IDS is a managed service that aids in detecting certain malware, spyware, command-and-control attacks, and other network-based threats.

Cloud Interconnect

Cloud Interconnect offers enterprise-grade connections to Google Cloud Platform. This solution provides direct connection between on-premise networks and GCP Virtual Private Cloud.

Cloud Load Balancing

Cloud Load Balancing is a distributed, software-defined, managed service for all traffic (HTTP(S), TCP/SSL, and UDP) to computing resources. Cloud Load Balancing rapidly responds to changes in traffic, network, backend health and other related conditions.

Cloud Network Address Translation (NAT)

Cloud Network Address Translation (NAT) enables virtual machine instances in a private network to communicate with the Internet, without external IP addresses.

Cloud NGFW

Cloud NGFW is a fully distributed, cloud-native firewall service that evaluates incoming and outgoing traffic on a network, according to user-defined firewall rules in the policy.

Cloud Router

Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between a Virtual Private Cloud (VPC) network and an external network, typically an on-premise network.

Cloud Service Mesh

Cloud Service Mesh is a service mesh available on Google Cloud and across supported GKE Enterprise platforms. It supports services running on a range of computing infrastructures. Cloud Service Mesh is controlled by APIs designed for Google Cloud, for open source, or for both.

bernard@botmaker.io

Google Confidental Information

Cloud Virtual Private Network (VPN)

Cloud Virtual Private Network (VPN) provides connections between on-premises or other external networks to Virtual Private Clouds on GCP via an IPsec connection or can be used to connect two different Google managed VPN gateways.

Google Cloud Armor

Google Cloud Armor provides access control configurations and at-scale defenses to help protect infrastructure and applications against distributed denial-of-service (DDoS), application-aware and multi-vector attacks.

Network Connectivity Center

Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud that facilitates connecting a customer's resources to its cloud network.

Network Intelligence Center

Network Intelligence Center provides a single console for managing Google Cloud's comprehensive network monitoring, verification, and optimization platform across the Google Cloud, multi-cloud, and on-premises environments.

Network Service Tiers

Network Service Tiers enable the selection of different quality networks (tiers) for outbound traffic to the Internet: Standard Tier primarily utilizes third-party transit providers while Premium Tier leverages Google's private backbone and peering surface for egress.

Service Directory

Service Directory is a managed service that offers customers a single place to publish, discover and connect their services in a consistent way, regardless of their environment. Service Directory supports services in Google Cloud, multi-cloud and on-premises environments and can scale up to thousands of services and endpoints for a single project.

Spectrum Access System

Spectrum Access System enables users to access the Citizens Broadband Radio Service (CBRS) in the United States, the 3.5 GHz band that is available for shared commercial use. Users can use Spectrum Access System to register CBRS devices, manage CBRS deployments, and access a non-production test environment.

Traffic Director

Traffic Director is Google Cloud Platform's traffic management service for open-source service meshes.

bernard@bottmaker.io

Google Confidental Information

Google

Virtual Private Cloud (VPC)

Virtual Private Cloud is a comprehensive set of managed networking capabilities for Google Cloud resources including granular IP address range selection, routes and firewalls.

Operations

Cloud Logging

Cloud Logging is a hosted solution that helps users gain insight into the health, performance and availability of their applications running on Google Cloud Platform and other public cloud platforms. It includes monitor dashboards to display key metrics, define alerts and report on the health of cloud systems. The components of Cloud Logging that run on other public cloud platforms are not in scope for this report.

Cloud Monitoring

Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from certain Services, hosted uptime probes, application instrumentation, alert management, notifications and a variety of application components.

Cloud Profiler

Cloud Profiler continuously gathers and reports source-level performance information from production services. It provides key information to determine what functions in code consume the most memory and CPU cycles so insights can be gained on how code operates to improve performance and optimize computing resources.

Cloud Trace

Cloud Trace collects latency data from applications and displays it in the Google Cloud Platform Console. It automatically analyzes trace data to generate in-depth performance reports that help identify and locate performance bottlenecks.

Google Cloud Backup and DR

Google Cloud Backup and DR is a managed backup and disaster recovery service for centralized protection of workloads in Google Cloud.

Personalized Service Health

Personalized Service Health, which lets users identify Google Cloud service disruptions relevant to user's projects so users can manage and respond to them efficiently. These disruptions are called service health events, and are available in the Google Cloud console and a variety of integration points.

bernardo@hotmail.com

Google Confidental Information

Google

Security and Identity

Access Approval

Access Approval allows customers to approve eligible manual, targeted access by Google administrators to their data or workloads prior to access being granted.

Access Context Manager

Access Context Manager allows customer administrators to define attribute-based access control for projects, apps and resources.

Access Transparency

Access Transparency captures near real-time logs of certain manual, targeted accesses by Google personnel, and provides them via Cloud Logging accounts.

Assured Workloads

Assured Workloads provides functionality to create security controls that are enforced on customer cloud environment and can assist with compliance requirements (e.g. FedRAMP Moderate compliance).

Binary Authorization

Binary Authorization helps customers ensure that only signed and explicitly authorized container images are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.

Certificate Authority Service

Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Customers can use Certificate Authority Service to create certificate authorities using Cloud KMS keys to issue, revoke, and renew subordinate and end-entity certificates.

Certificate Manager

Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the certificates.

Chrome Enterprise Premium

Chrome Enterprise Premium is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware and phishing attacks. Chrome Enterprise Premium is an integrated platform incorporating cloud-based services and software components.

bernard@botmaker.io

Cloud Asset Inventory

Cloud Asset Inventory is a service that allows customers to view, monitor, and analyze cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.

Cloud External Key Manager (Cloud EKM)

Cloud EKM lets customers encrypt data in Google Cloud Platform with encryption keys that are stored and managed in a third-party key management system deployed outside Google's infrastructure.

Cloud Hardware Security Module (HSM)

Cloud HSM is a cloud-hosted Hardware Security Module (HSM) service for hosting encryption keys and performing cryptographic operations.

Cloud Key Management Service (KMS)

Cloud KMS is a cloud-hosted key management service that manages encryption for cloud services. It enables the generation, use, rotation, and destruction of encryption keys.

Firebase App Check

Firebase App Check provides a service that can help protect access to user's APIs with platform specific attestation that helps verify app identity and device integrity.

Firebase Authentication

Firebase Authentication is a fully managed user identity and authentication system providing backend services enabling sign-in and sign-up experiences for an application or service.

Google Cloud Identity-Aware Proxy

Google Cloud Identity-Aware Proxy (Cloud IAP) is a tool that helps control access to applications running on Google Cloud Platform based on identity and group membership.

Google Threat Intelligence

Google Threat Intelligence combines the unmatched depth of our Mandiant frontline expertise, the global reach of the VirusTotal community, and the breadth of visibility only Google can deliver, based on billions of signals across devices and emails. Google Threat Intelligence includes Gemini in Threat Intelligence, our AI-powered agent that provides conversational search across our vast repository of threat intelligence, enabling customers to gain insights and protect themselves from threats faster than ever before. The Attack Surface Management (ASM) and Digital Threat Monitoring (DTM) features of Google Threat Intelligence are Mandiant products and maintain equivalent certifications.

bernard@bothmaker.no

Google Confidental Information

Google Security Operations (SIEM)

Google Security Operations Security Information and Event Management (SIEM) enables enterprise security teams to detect, investigate, and respond to threats at speed and scale. Chronicle SIEM does this by collecting security telemetry data, aggregating it, normalizing it, and applying threat intelligence to identify the highest priority threats.

Google Security Operations (SOAR)

Google Security Operations Security Orchestration, Automation and Response (SOAR) is a platform designed to help organizations detect, investigate, and respond to security threats in real-time. The platform is powered by Google Cloud's infrastructure and leverages the machine learning capabilities of Google to automate and streamline security workflows.

GTI for Google Security Operations

GTI for Google Security Operations is a service extension for Google Security Operations (SIEM) that hunts for threats in external customer environments. This effort includes active research for new and emerging threats. It also includes focused batch hunting that extracts suspicious logs warranting either special review or logs that should be automatically sent to customers

Identity & Access Management (IAM)

Identity & Access Management (IAM) enables the administration and authorization of accesses to specific resources and provides a unified view into security policies across entire organizations with built-in auditing.

Identity Platform

Identity Platform is a customer identity and access management (CIAM) platform delivered by Google Cloud enabling organizations to add identity management and user security to their applications or services.

Key Access Justifications (KAJ)

Key Access Justifications (KAJ) provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at-rest to in-use.

Managed Service for Microsoft Active Directory (AD)

Managed Service for Microsoft Active Directory (AD) is a Google Cloud service running Microsoft AD that enables customers to deploy, configure and manage cloud-based AD-dependent workloads and applications. It is a fully managed service that is highly available, applies network firewall rules, and keeps AD servers updated with Operating System patches.

Privileged Access Manager

Privileged Access Manager (PAM) allows customers to control just-in-time temporary privilege elevation for select principals, and to view audit logs afterwards to find out who had access to what and when.

bernard@botmaker.io

Google Confidental Information

Organization Policy

Organization Policy provides customizable security guardrails to centrally enforce resource configuration compliance across resource hierarchies.

reCAPTCHA Enterprise

reCAPTCHA Enterprise helps detect fraudulent activity on websites using risk analysis techniques to distinguish between humans and bots.

Resource Manager API

Resource Manager API allows users to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects) to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization enables users to manage common aspects of resources such as access control and configuration settings.

Risk Manager

Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including CIS benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.

SecLM

SecLM or more specifically, the SecLM Platform (formerly known as Security AI Workbench or SAW) - refers to the API and platform that we've built based on the SecPaLM models. The platform orchestrates reasoning, extensions, retrieval augmented generation (RAG), and other techniques to leverage authoritative security data from sources, like Mandiant Advantage Threat Intelligence (MATI) and VirusTotal, and deliver the highest quality responses to security-related prompts.

Secret Manager

Secret Manager provides a secure method for storing API keys, passwords, certificates, and other sensitive data.

Security Command Center

Security Command Center is a log monitoring and security scanning tool that generates analytics and dashboards to help customers to prevent, detect, and respond to Google Cloud security and data threats.

Sensitive Data Protection (including Cloud Data Loss Prevention)

Sensitive Data Protection is a fully-managed service enabling customers to discover, classify, de-identify, and protect sensitive data, such as personally identifiable information.

VirusTotal

VirusTotal enables organizations to research and hunt for malware, to investigate security incidents, to automate analysis, and to keep user investigations private and secure.

bernard@bottmaker.io

Google

VPC Service Controls

VPC Service Controls provides administrators with the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks.

Web Risk API

Web Risk API is a Google Cloud service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.

Serverless Computing

Cloud Functions

Cloud Functions is a serverless compute solution that runs single-purpose functions in response to GCP events and HTTP calls (webhooks). Cloud Functions can be triggered asynchronously by Cloud Pub/Sub, Cloud Storage, GCP infrastructure events, and Firebase products. Cloud Functions scales automatically to meet request load and the user does not need to manage servers or the runtime environment.

Cloud Functions for Firebase

Cloud Functions for Firebase are developer tools used for development and deployment of Google Cloud Functions. Cloud Functions enable developers to run their own backend code that executes automatically based on HTTP requests and Firebase and Google Cloud Platform events. Developers' functions are stored in Google’s cloud and run in a managed Node.js environment.

Cloud Run

Cloud Run (fully managed) is a serverless, managed compute platform that automatically scales stateless HTTP containers, running requests or event-driven stateless workloads. Cloud Run provides the flexibility to run services on a fully managed environment.

Cloud Scheduler

Cloud Scheduler is a fully managed enterprise-grade cron job scheduler. It allows customers to schedule jobs, including batch, big data jobs, cloud infrastructure operations, and more. It also acts as a single interface for managing automation tasks, including retries in case of failure to reduce manual toil and intervention.

Cloud Tasks

Cloud Tasks is a fully managed service that allows customers to manage the execution, dispatch, and delivery of a large number of distributed tasks.

Datastream

Datastream is a serverless and easy-to-use change data capture (CDC) and replication service that allows users to synchronize data streams across heterogeneous databases and applications

bernard@hotmail.io

Google Confidental Information

reliably and with minimal latency. Datastream supports streaming changes to data from Oracle and MySQL databases into Cloud Storage.

Eventarc

Eventarc is a fully managed service for eventing on Google Cloud Platform. Eventarc connects various Google Cloud services together, allowing source services (e.g., Cloud Storage) to emit events that are delivered to target services (e.g., Cloud Run or Cloud Functions).

Workflows

Workflows is a fully managed service for reliably executing sequences of operations across microservices, Google Cloud services, and HTTP-based APIs.

Storage

Backup for GKE

Backup for GKE enables data protection for workloads running in Google Kubernetes Engine clusters.

Cloud Filestore

Cloud Filestore is a service for fully managed Network File System (NFS) file servers for use with applications running on Compute Engine virtual machines (VMs) instances or Google Kubernetes Engine clusters.

Cloud Storage

Cloud Storage is Google Cloud Platform's unified object/blob storage. It is a RESTful service for storing and accessing data on Google Cloud Platform's infrastructure. It combines the simplicity of a consistent API and latency across different storage classes with reliability, scalability, performance and security of Google Cloud Platform.

Cloud Storage for Firebase

Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for Firebase apps. Cloud Storage for Firebase is backed by Cloud Storage, a service for storing and accessing data on Google's infrastructure.

Parallelstore

Parallelstore is a parallel file system for high-performance computing and AI/ML workloads. Built on the Distributed Asynchronous Object Storage (DAOS) architecture, Parallelstore combines a fully distributed metadata and key-value architecture to deliver high-performance throughput and IOPS.

bernard@buttmaker.io

Google Confidental Information

Google

Persistent Disk

Persistent Disk provides a persistent virtual disk for use with Google Compute Engine and Google Kubernetes Engine compute instances. It is available in both SSD (Solid State Drive) and HDD (Hard Disk Drive) variations.

Other

Cloud Billing

Cloud Billing provides methods to programmatically manage billing for projects on the Google Cloud Platform.

Google Earth Engine

Google Earth Engine combines a multi-petabyte catalog of satellite imagery and geospatial datasets with planetary-scale analysis capabilities. Scientists, researchers, and developers can use Earth Engine to detect changes, map trends, and quantify differences on the Earth's surface.

Google Cloud Marketplace

Google Cloud Marketplace offers ready-to-go development stacks, solutions, and services from third-party partners and Google to accelerate development. It enables the deployment of production-grade solutions, obtains direct access to partner support, and receives a single bill for both GCP and third-party services.

Google Cloud Skills Boost

Google Cloud Skills Boost is where you can access Google Cloud’s entire catalog of labs and courses. Customer end users can discover learning paths, build in-demand cloud skills, track your activity progress, and validate your knowledge with badges.

Tables

Tables is a lightweight collaborative database to help organize and automate tasks or processes for small teams and businesses.

Data Centers

The above products are serviced from data centers operated by Google around the world. Below is a list of Google's production data center locations that host the above products and operations for Google Cloud Platform. The scope of this report does not cover Google edge points of presence (PoPs).

North America, South America

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America

bernard@bormakerio

Google

- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Austin (TX), United States of America**
- Chandler (AZ), United States of America
- Clarksville (TN), United States of America
- Columbus (1) (OH), United States of America
- Columbus (2) (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Gainesville (VA), United States of America
- Guanajuato, Mexico
- Henderson (NV), United States of America
- Lancaster (OH), United States of America
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Los Angeles (3) (CA), United States of America
- Markham, Ontario, Canada
- Midlothian (1) (TX), United States of America
- Midlothian (2) (TX), United States of America*
- Midlothian (3) (TX), United States of America***
- Moncks Corner (SC), United States of America
- Montreal (1), Quebec, Canada
- Montreal (2), Quebec, Canada
- New Albany (OH), United States of America
- Omaha (NE), United States of America
- Osasco, Brazil
- Papillion (NE), United States of America
- Phoenix (AZ), United States of America
- Pryor Creek (OK), United States of America
- Quilicura (1), Santiago, Chile
- Quilicura (2), Santiago, Chile
- Quilicura (3), Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America
- Salt Lake City (3) (UT), United States of America

bernal@hotmaker.io

Google

- San Bernardo, Santiago, Chile
- Santana de Parnaíba, Brazil
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- The Dalles (3) (OR), United States of America**
- Toronto (1), Ontario, Canada
- Toronto (2), Ontario, Canada
- Vinhedo, Brazil
- Widows Creek (AL), United States of America

Europe, Middle East, and Africa

- Berlin (1), Germany
- Berlin (2), Germany
- Berlin (3), Germany
- Dammam, Saudi Arabia
- Dammam (2), Saudi Arabia*
- Dammam (3), Saudi Arabia*
- Dalarna, Sweden
- Doha (1), Qatar
- Doha (2), Qatar
- Doha (3), Qatar
- Dublin, Ireland
- Eemshaven, Groningen, The Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany
- Frankfurt (8), Hesse, Germany
- Frankfurt (9), Hesse, Germany**
- Fredericia, Denmark
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- Johannesburg (1), South Africa
- Johannesburg (2), South Africa
- Johannesburg (3), South Africa
- London (1), United Kingdom
- London (3), United Kingdom

bernard@botmaker.io

Google

- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Middenmeer, Noord-Holland, The Netherlands
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland

bernard@botmaker.io

Asia Pacific

- Changhua, Taiwan
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India
- Delhi (4), India***
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai City, Chiba, Japan
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Jakarta (3), Indonesia

Google Confidental Information

Google

- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Lok Yang Way, Singapore
- Loyang, Singapore
- Melbourne (1), Victoria, Australia
- Melbourne (2), Victoria, Australia
- Melbourne (3), Victoria, Australia
- Mumbai (1), India
- Mumbai (2), India
- Mumbai (3), India
- Mumbai (4), India
- Mumbai (5), India***
- Osaka (1), Japan
- Osaka (2), Japan
- Seoul (1), South Korea
- Seoul (2), South Korea
- Seoul (3), South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Sydney (4), NSW, Australia
- Wenya, Singapore

bernard@botmaker.io

* Indicates data center is in scope only for the period 1 November 2024 through 31 July 2025

** Indicates data center is in scope only for the period 1 March 2025 through 31 July 2025

*** Indicates data center is in scope only for the period 1 May 2025 through 31 July 2025

B. Relevant Aspects of Internal Control

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

- **Control Environment:** Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure
- **Information and Communication:** Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control its operations

- **Risk Assessment:** The entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed across the internal and external control environment, including third-party risk
- **Monitoring Activities:** The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant
- **Control Activities:** Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's control objectives are effectively carried out

This section briefly describes the four (4) essential characteristics and other interrelated components of internal controls that support the achievement of the applicable trust services principles and criteria for security, availability, confidentiality, and privacy as it pertains to the Google Cloud Platform products that may be relevant to customers into four broad areas:

- Policies (Control Environment and Risk Assessment) – The entity has defined and documented its policies relevant to the particular principle
- Communications (Information and Communication) – The entity has communicated its defined policies to responsible parties and authorized users of the system
- Procedures (Control Activities) – The entity placed in operation procedures to achieve objectives in accordance with its defined policies
- Monitoring (Monitoring Activities) – The entity monitors the system and takes action to maintain compliance with its defined policies

With respect to internal controls and relevant customers, Google defines Customers as enterprise users that have entered into an agreement, under which Google has agreed to provide Google Cloud Platform services as a data processor.

bernard@bottmaker.no

C. Policies

Internal Control Environment

Google has designed its internal control environment with the objective of providing reasonable, but not absolute, assurance as to the security, availability, confidentiality, and privacy of financial and user information, as well as the protection of assets from unauthorized use or disposition. Management has established and maintains an internal control structure that monitors compliance with established policies and procedures.

Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, confidentiality, and privacy controls.

To maintain internal compliance, Google has established a disciplinary process for non-compliance with the Code of Conduct, security and privacy policies, and other personnel requirements which could include dismissal, lawsuits, and/or criminal prosecution.

The organization utilizes technologies to support the workforce in both remote and office work environments.

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Google Cloud Platform System. Commitments to customers are communicated via Terms of Service, Google Cloud Platform System Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

System Requirements

Google has established internal policies and processes to support the delivery of Google Cloud Platform System products to customers. These internal policies are developed in consideration of legal and regulatory obligations, to define Google's organizational approach and system requirements.

The delivery of these services depends upon the appropriate internal functioning of system requirements defined by Google to meet customer commitments.

The following processes and system requirements function to meet Google's commitments to customers with respect to the terms governing the security and privacy of customer data:

- **Access Security:** Google maintains data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege
- **Change Management:** Google requires standard change management procedures to be applied during the design, development, deployment, and maintenance of Google applications, systems, and services
- **Incident Management:** Google monitors security event logs and alerts to determine the validity of security or privacy threats. Potential threats, including threats related to security and privacy are escalated to the appropriate team including incident management. Google's dedicated security personnel will promptly investigate and respond to potential and known incidents
- **Data Management:** Google complies with any obligations applicable to it with respect to the processing of Customer Personal Data. Google processes data in accordance with Google Cloud Platform Terms of Service and/or Data Processing Agreements, and complies with applicable regulations
- **Data Security:** Google maintains data security and privacy policies and implements technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Google takes appropriate steps to help ensure compliance with the security measures by its employees, contractors, and vendors to the extent applicable to their scope of performance

bernard@hotmail.com

Google Confidental Information

- **Third-Party Risk Management:** Google conducts an assessment of the security and privacy practices of third-party suppliers to help ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Google conducts routine inspections of subprocessors to help ensure their continued compliance with the agreed upon security and privacy requirements. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from suppliers to comply with these practices.

Internal Functions and Policies

Google has established company structures and reporting lines and has helped ensure sufficient authorities are available to support compliance activities with regulatory, legal, contractual, and privacy requirements. Formal organizational structures exist and are available to Google personnel on the Company's intranet. The intranet provides drill-down functionality for identifying personnel in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Google has also developed the Data Security Policy, Data Classification Guidelines and Security Labels for Google Information and Privacy policies to establish procedures for information labeling and handling in accordance with the Google guidelines. Additionally, Google maintains policies that define the requirements for the use of cryptography and policies for securing mobile devices to help ensure company and customer data are protected. Security and Privacy policies are reviewed annually, and other materials derived from policies, like guidelines, frequently asked questions (FAQs), and other related documents are reviewed and updated as needed.

D. Communications

Information and Communication

To help align its business strategies and goals with operating performance and controls, Google has implemented various methods of communication to help ensure that all interested parties and personnel understand their roles and responsibilities and to help ensure that significant events are communicated in a timely manner. These methods include:

- Orientation and training programs for newly hired employees
- An information security and privacy training program that is required to be completed by relevant personnel annually
- Organization personnel are required to acknowledge the code of conduct
- Regular management meetings for updates on business performance and other business matters
- Company goals and responsibilities are developed and communicated by management on a periodic basis and amended as needed. Results are evaluated and communicated to employees

bernal@pennker.it

- Detailed job descriptions; product information (including system and its boundaries); and Google's security, availability, confidentiality, and privacy obligations that are made available to employees in the intranet
- The use of electronic mail messages to communicate time-sensitive messages and information
- Publishing security and privacy policies and security-related updates on the intranet, which is accessible by all Google employees, temporary workers, contractors, and vendors

Google has communicated to employees and extended workforce (i.e., temporary workers, vendors, and contractors) instructions and mechanisms for reporting potential security and privacy concerns or incidents. Google has also implemented various methods of communication to help ensure that user entities understand Google's commitments to security, availability, confidentiality, and privacy for Google Cloud Platform; and to help ensure that significant events are communicated to user entities in a timely manner. The primary conduit for communication is the Google website, which is made available to all user entities. This includes blog postings on the Official Google Blog and various product specific blogs support forums, and release notes. Google provides 24 x 7 assistance, including online and phone support to address customers' concerns. Customer service and/or technical support representatives are also an important communication channel, as they maintain records of problems reported by the user entity. Customer service representatives also assist in communicating information regarding new issues and/or developments, changes in services, and other information. Additionally, Google maintains an established Board of Directors that operates independently from management. The Board exercises oversight over management decisions.

As a data processor, Google limits processing to what is specified in the contracts with the controller or as otherwise required under applicable data protection laws. Customer data is processed in accordance with the Data Processing Addendum and is externally published (see https://cloud.google.com/terms/data-processing-terms). As data controllers, customers are responsible for communicating choices available to users regarding collection, use, retention, disclosure and disposal of personal information. Google does provide customers with mechanisms to access, modify, delete, and export customer data.

E. Procedures

Hiring Practices

Google has designed formal global hiring practices to help ensure that new, rehired, or transferred employees are qualified for their functional responsibility. Every employee has a written job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Google. Where local labor law or statutory regulations permit, Google may conduct criminal, credit, and/or security checks on all potential employees, temporary workers, and independent contractors, as well as verification of the individual's education, previous employment, and referrals. The specifics or extent of background checks performed depend on the position and location for which the individual is applying.

Upon acceptance of employment, all employees including extended workforce personnel are required to execute a confidentiality agreement as well as acknowledge receipt and compliance with Google's Code of Conduct. The confidentiality and privacy of customer data is emphasized in the handbook and also during new employee orientation. It is the responsibility of every employee to timely communicate significant issues and exceptions to an appropriate higher level of authority within the Company.

Risk Management

Risk management is a pervasive component of Google Cloud Platform System's products provided by Google to user entities, irrespective of the location or business area. The Google teams which lead engineering, sales, customer service, finance, and operations have the primary responsibility to understand and manage the risks associated with their activities for user entities using Google Cloud Platform's products. These risk management and mitigation activities have been integrated into Google's repeatable process models.

At a corporate level, there are multiple functional areas, Legal, Information Security, Internal Audit, Global Directive Assurance (performing first party audit), Privacy Engineering, Compliance Assurance and Advisory, CSRM (Compliance, Security, and Risk Management), Ethics and Business Integrity, RCI (Risk, Compliance and Integrity), Regulatory Affairs, and PSS (Privacy, Security and Safety), that provide risk management support through policy guidelines and internal consulting services.

Google develops and maintains a risk management framework to manage risk to an acceptable level for Google Cloud Platform. Google has developed vulnerability management guidelines and regularly analyzes the vulnerabilities associated with the system environment. Google takes into consideration various threat sources such as insider attacks, external attacks, errors and omissions, and third-party related issues such as inadvertent disclosure of Google confidential information (for example, payroll data) by a third party.

Factors including threat-source motivation and capability, the nature of the vulnerability, and existence and effectiveness of current controls are considered in determining the probability that a potential vulnerability may be exposed. The likelihood that a potential vulnerability could be exposed by a given threat-source is designated by Google as high, medium, or low.

Google then determines the potential adverse impact resulting from a successful exploitation of vulnerabilities. The highest priority is given to any potential compromise of user data.

The level of risk and remediation priority for a particular threat/vulnerability pair is expressed as a function of:

- The likelihood of a given threat-source's attempt to exploit a given vulnerability
- The impact should a threat-source successfully expose the vulnerability
- The effectiveness of existing security and privacy controls for mitigating risk

Google performs formal risk assessments for each of their in scope product areas at least annually and determines the likelihood and impact of identified risks, using qualitative and quantitative

methods. The likelihood and impact associated with each risk is determined independently, considering each risk category. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management. Management also proactively identifies emerging risks for product areas to include within their respective risk assessments.

Google has an established Internal Audit function and compliance specialists responsible for evaluating the effectiveness of controls in addressing a given risk, including, among other controls, identity management, source code management, and authentication infrastructure controls against requirements. They perform risk-based assessments and issue audit reports regarding their analysis. Remediation of security and privacy deficiencies are tracked through internal tools and remediation plans.

Third-Party Risk Management

Google may utilize third-party vendors to support Google Cloud Platform. Prior to onboarding, Google completes the nondisclosure agreement (NDA) then performs the vendor security assessments (VSA) on all vendors with whom Google shares confidential or sensitive information, including user data. A VSA is an important health check of a vendor's operational security posture. It assesses if a vendor adheres to generally accepted security and data protection best practices. The outcome of a VSA is a risk assessment and an approval that determines if a vendor should or can be used. At a high level, each of these assessments involves:

- An initial risk assessment to determine if a VSA is required or not such as instances where vendors handle, collect, or access any User Data, or Business Data that is classified as Need-to-Know
- A risk-based review of the policies, processes, and controls the vendor has in place compared to generally accepted security best practices using questionnaire-based information gathering
- A tailored risk assessment for Mergers and Acquisitions due diligence or third-party risk management in partnerships, joint ventures, and other complex relationships.
- Reviewing and citing independent verification of the security state of systems relevant to Google's use of the vendor

A subset of vendors are considered to be subprocessors based on the data sharing relationship between the vendor and Google. Google utilizes subprocessors to support Google Cloud Platform, and has established expectations for subprocessors related primarily to security and privacy. The meeting of these expectations are subject to periodic review by Google. However, subprocessors do not manage or perform any Google Cloud Platform controls tested herein.

Google maintains a Subprocessor Audit Program that is tasked with the periodic information security and privacy assessment of subprocessors using ISO 27001 as the baseline. Google evaluates conformance to these expectations through inspection of third-party ISO certifications, SOC 2 reports, or onsite/virtual inspections. In the case that Google identifies any deviations in the performance of subprocessor controls, findings are evaluated by Google and discussed with the subprocessors upon completion of the audit. When applicable, remediation plans are put in place to timely resolve issues.

bernard@bottomaker.io

Google has also implemented a Subprocessor Data Processing Agreement (SDPA) to contract with subprocessors. The SDPA defines the security and privacy obligations which the subprocessor must meet to satisfy Google's obligations regarding customer data, prior to Google granting such access. Per the Data Processing Addendum, Google notifies the customer prior to onboarding a new subprocessor. Information about the subprocessor including function and location is externally published (see https://cloud.google.com/terms/subprocessors).

Data Confidentiality and Privacy

Google has established training programs for privacy and information security to support data confidentiality and privacy. Relevant Google personnel are required to complete these training programs within 90 days of joining the organization and annually thereafter. All new product and product-feature launches that include collection, processing, or sharing of user data are required to go through an internal security and privacy design review process. These reviews are performed by the security, legal, and privacy teams. Databases and websites exist to track and monitor progress of Google Cloud Platform project developments. In addition to the preventative controls, Google has also established detective measures to investigate and determine the validity of security threats. In the case of an incident there are incident response processes to report and handle events related to topics such as security and confidentiality. Google establishes confidential agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchange with external parties.

For government agency data requests, Google has mechanisms in place to record and track transfers and disclosures of users data to third parties. Customers are notified of third party data requests in accordance with any procedure and time period agreed in the contract, unless such disclosure is prohibited by law. As a data processor, Google limits disclosures of customer data to disclosures that are legally required or authorized by the data controller.

Information Security Program

Google's Information Security program is designed to safeguard information assets against unauthorized use, disclosure, modification, damage, or loss. The program includes educating Google personnel about security related issues, assessing current policies and developing new policies, assisting in strengthening technical measures to protect corporate resources, and developing mechanisms to react to incidents and events that could affect Google's information assets.

Google has dedicated security teams responsible for educating Google personnel about security and assisting product teams with security design. Information security is managed by a dedicated Security and Privacy executive who is independent of Information Technology management responsibilities and may escalate security issues or concerns directly to the board. The Security Team also reviews the security practices of vendors and the security posture of vendor products for all vendors that Google shares confidential or sensitive information with.

Google has security policies that have been reviewed and approved by management and are published and communicated to employees and extended workforce with access to the Google

Google Confidental Information

intranet. Google's security policies describe security objectives, provide a security framework, and emphasize the importance of security to Google's business.

Information Privacy Program

Google's Information Privacy program is designed to safeguard information assets against unauthorized use, access, disclosure, modification, damage, or loss, as well as the privacy of customer data. The program includes, but is not limited to, developing and managing privacy policies, developing privacy requirements for products and services including reviewing data usage to help ensure processing of customer data is in accordance with the applicable data protection agreements entered into between Google and customers based on applicable data protection laws and regulations, and developing mechanisms to react to privacy incidents and events that could affect Google's information assets and customer data. Google has dedicated privacy teams responsible for educating Google personnel about privacy, assisting product teams with privacy design, and overseeing privacy practices at the company. Google has privacy policies that have been reviewed and approved by management and are published and communicated to employees and vendors with access to the Google environment. Google's privacy policies describe privacy objectives, provide a privacy framework and required practices, and emphasize the importance of privacy to Google's business.

Google's role as a data processor and the scope of the processing are defined in the applicable Data Processing Addendum (see https://cloud.google.com/terms/data-processing-terms)

Network Architecture and Management

The Google Cloud Platform system architecture utilizes a fully redundant network infrastructure. Border routers that provide the connection point between Google Cloud Platform and any Internet Service Providers are designed to run in a redundant configuration. Where border routers are in use, firewalls are also implemented to operate in a redundant configuration.

Google has implemented perimeter devices to protect the Google network from external network attacks and configurations of perimeter devices are centrally managed. Google segregates networks based on the types of services, users, and information systems. The network is managed via specialized tools. Google employs automated tools to inventory network devices and machines. Authorized security and network engineers access the network devices (production routers and switches) to monitor, maintain, manage, and secure the network through these tools.

Network monitoring mechanisms are in place to detect and disconnect access to the Google network from unauthorized devices. Google has documented procedures and checklists for configuring and installing new servers, routers and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet.

Google has a firewall configuration policy that defines acceptable ports that may be used on a Google firewall. Only authorized services and protocols that meet Google's requirements are

bernard@bdtmaker.ro

permitted access to the network. The firewalls are designed to automatically deny all unauthorized packets not configured as acceptable. Administrative access to the firewalls is limited to authorized administrative personnel using the Secure Shell (SSH) protocol and two-factor authentication. Changes to network configurations are peer reviewed and approved prior to deployment. Google has implemented automated controls on network devices to identify distributed denial of service (DDOS) attacks. Google has established incident response processes to report and handle such events (see the Incident Management section).

Authentication, Authorization, and Administration

Authentication and access controls are implemented to restrict access to Google Cloud Platform production systems, internal support tools, and customer data. Machine-level access restriction relies on Google-developed distributed authentication service based on Transport Layer Security (TLS) and Secure Sockets Layer (SSL) certificates which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google uses encryption to secure user data in transit between Google production facilities. Access to internal support tools, those used by Google operational staff to maintain and troubleshoot the systems for Google Cloud Platform is controlled via Access Control Lists (ACLs) thus limiting the use of these tools to only those individuals that have been specifically authorized.

Digital certificates used for machine authentication and data encryption are issued by an internal Google certificate authority. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to the Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication.

Google follows a formal process to grant or revoke personnel access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system that utilizes Secure Shell (SSH) and TLS/SSL certificates help provide secure and flexible access. These mechanisms are designed to grant access rights to systems and data only to authorized users. Additionally, access requests via "on demand" mechanisms are reviewed and approved by an authorized second individual prior to being granted and the event is logged.

Both user and internal access to customer data are restricted through the use of unique user account IDs and via the Google Accounts Bring Your Own Identity (BYOID) system for external users. Access to sensitive systems and applications requires two-factor authentication in the form of unique user IDs, strong passwords, security keys, and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data (and other need-to-know data) is appropriate and authorized. Access to production machines, network devices and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semiannual basis under the direction of the group administrators, and any inappropriate access is removed.

Access authorization in Google Cloud Platform is enforced at all relevant layers of the system. The granting or modification of access rights is based on the user’s job responsibilities or on a need-to-know basis and must be authorized and approved by the user’s functional manager or

Google Confidental Information

system owners. Approvals are managed by workflow tools and are logged. Production system access is only granted to individuals who require this level of access to perform necessary tasks. Additionally, all users with access to production systems are required to complete security and privacy training annually. Access to individual production systems via critical access groups is reviewed on a periodic basis by the system owners and inappropriate access is removed for Google personnel who no longer have a business need for such access. Access to all corporate and production resources are automatically removed upon submission of a termination request by the manager of any departing employee, temporary worker, contractor or vendor, or by the appropriate Human Resources manager.

Password Guidelines

Google personnel are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection, and management guidelines, which enforce the following:

- Minimum length
- Complexity
- History
- Idle time lockout setting

Password configuration requirements are enforced by internal systems. In addition to the security requirements enforced during configuration, internal passwords are subject to cryptographic hashing to mitigate the risk of unauthorized disclosure or modification.

Google has supplemented passwords with a two-factor authentication requirement for internal personnel to access sensitive internal corporate and production services and to access Google Cloud Platform in the production environment from the corporate network. Two-factor authentication provides additional protection to prevent user account manipulation in case the user's password is compromised.

Google Cloud Platform end users can also authenticate in one of three ways:

- Using their user ID and a password that is managed by Google
- Using a two-step authentication process that includes their user ID, password, and a security key
- Through the Security Assertion Markup Language (SAML) based Single Sign-On (SSO) process which uses the user entity's own account management system to authenticate users and a certificate with an embedded public key, which is registered with Google for each customer entity

Physical Access — Data Center Physical Security

Google maintains consistent policies and standards across its data centers for physical security to help protect production servers, network devices, and network connections within Google data centers. Guidelines for evaluating the security of data centers are described in Google's data center security evaluation criteria. Additionally, data center personnel perform periodic surveys

bernard@hotmaker.io

and reviews of data centers. Data centers that house Google Cloud Platform systems and infrastructure components are reviewed and assessed periodically for ongoing security compliance. A security report is then created summarizing any observations, deviations, or action items. This report is presented to executive management for review and approval. Corrective actions are taken when necessary. The data center security evaluation criteria elements include:

- Existence of security guards, access badges, and video cameras
- Entrances, cages, suites, and rooms in use by Google are secured by either badge readers, secondary identification mechanisms, and/or physical locks
- Emergency exit points from server rooms are alarmed
- Video cameras exist to monitor the interior and exterior of the facility
- 24 x 7 on-site security personnel

Formal access procedures exist for allowing physical access to the data centers. There are documented procedures for issuing badges to staff and/or visitors and the owner of each badge is tracked and documented. All entrants to the data center, whether they are Google employees, visitors, or contractors, must identify themselves as well as show proof of identity to Security Operations.

Valid proof of identity consists of (1) a photo ID issued by Google or (2) a governmental entity. Only validated visitors and authorized Google employees and contractors are permitted to enter the data centers. Authorized Google Data Center Approvers must approve all visitors in advance for the specific data center and internal areas they wish to visit.

After the individual's access authorization is verified, the visit is logged, and access is granted for the specified dates and times. These logs are retained by Google security for review as needed. Visitors are provided a temporary badge and must be escorted by an authorized Google employee to access areas beyond the lobby. When the visitors leave the data center, they must return the visitor badge.

Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas. Google authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items. Google also utilizes automated mechanisms to track inventory of all production machines and inventory of all serialized server components. Only authorized Google employees or contractors permanently working at the data centers are permitted to request standing access to the facility areas needed for their role and responsibilities. Data center access requests must be made through internal tools and require the approval of authorized data center personnel. All other Google employees and authorized contractors requiring temporary data center access must also have an approved access request and register at the guard station upon arrival. User access lists to high-security areas in data centers are reviewed on a quarterly basis and inappropriate access is removed in a timely manner.

Data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network infrastructure are connected to redundant power sources that are

bernard@formaler.io

physically protected from disruption and damage in addition to emergency power which is available in the event of a loss of power. Google performs preventative and regular maintenance on fire detection and protection equipment, Uninterruptible Power Supply (UPS), generators, HVAC, and emergency lighting systems. Please refer to Section **A. Overview of Operations** above for a list of Google's data center locations.

Change Management

Changes to Google Cloud Platform are delivered as software releases through three (3) pipelines:

- Product functionality changes or builds related to the service running in Google's production environment;
- Images, downloads, or software updates are made available to customers; and
- Open source code packages maintained in a public source code repository.

Changes including configuration changes, code modifications, and new code creation, follow this change management process. Change Management policies and guidelines, including code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented. Each service has documented release processes that specify the procedures to be used, including definition of the scope of changes to be delivered, source code control, code review, building, testing, and record keeping. Development, testing, and build environments are separated from the production environment through the use of logical security controls.

The change process starts with a developer checking out a copy of source code files from the source code management system to modify them. Once development is complete, the developer initiates applicable testing and code reviews. Once the change has received the appropriate code review, the change can be submitted making it the new head version. Google requires that production code reviewers be independent of the developer assigned to the change and follows Google coding standards, in accordance with their policy. Production code reviews are systematically enforced. Emergency changes to production environments must have a valid justification and are logged, monitored and reviewed.

If needed, once the code is submitted, it can be used to build packages or binaries. During the build process, code is subject to automated testing, the results of which are monitored by engineers. Successfully built packages or binaries can be migrated to staging or QA environments where they can be subject to additional review. When the approved change is ready for deployment to production, it is deployed in a controlled manner, with monitoring in place to notify engineers of anomalies in the deployment. The process from build to release is aided by several tools that automate tasks, including testing and deployment. Employees at Google have the ability to view changes, however, access to modify code and approve changes is controlled via functionality of internal tools that support the build and release process. Changes to customer facing services that may affect confidentiality, processing integrity, and/or availability are communicated to relevant personnel and impacted customers. Please note, implementations and customizations by end-user customers after source code has been made available by Google in the public repositories are out of scope.

bernard@bonnaker.io

Google Confidental Information

Guidelines are made available internally to govern the installation of software on organization-owned assets. Additionally, tools are utilized to detect deviations from pre-defined Operating System (OS) configurations on production machines and correct them automatically. This allows for an easy roll out of updates to system files in a consistent manner and helps ensure that machines remain in a known current state.

Vulnerability Management

The goal of Google's Vulnerability Management program is to investigate and respond to all relevant security vulnerabilities. The Vulnerability Management Guidelines describe how vulnerabilities are detected, classified, and remediated at Google. As part of this program, the security operations team conducts network vulnerability scans to detect vulnerabilities in software, systems, and network devices. These scans are conducted on an ongoing basis, to identify and remediate potential vulnerabilities.

Also, external third-party penetration tests are performed on an annual basis for a predetermined subset of the services included in the Google Cloud Platform System, and corrective actions are taken as necessary. The subset of services included in any given year are determined by the Google Security and the Office of Compliance & Integrity teams and is based on their understanding of the organization's current risk environment, as well as the organization's current regulatory and compliance requirements.

Incident Management

Dedicated on-call personnel and incident response teams are responsible for managing, responding to, and tracking incidents. These teams are organized into formalized shifts and are responsible for helping resolve emergencies 24 x 7. Incident response policies are in place and procedures for handling incidents are documented.

Incident Alert and Recording

Automated signals generate alerts whenever an anomaly occurs. Production monitoring tools, in response to an anomaly, automatically generate alerts to relevant teams. An anomaly may also be manually documented by Google personnel when an issue is identified or in response to a customer service request or reported through externally available channels. Production systems are configured to send system events to monitoring and alerting tools. Google personnel use these tools to respond to potential incidents, including security and privacy incidents.

Alerts capture information necessary for initial response (e.g., origin, service description, impacted area, etc.). Alerts are addressed by relevant teams to identify if the anomaly indicates an issue or potential issue. If necessary, incidents are created for alerts that require additional investigation. Additional details can be added to the incident to supplement the initial alert(s). The incident is assigned an initial severity level to prioritize mitigation efforts to incidents of greatest impact. Each severity level has been formally defined to capture the importance of each incident/problem type. There are established roles and responsibilities for personnel tasked with incident management, including the identification, assignment, managed remediation, and communication of incidents.

bernard@bottmaker.io

Google

Incident Escalation

Google has documented escalation procedures and communication protocols that address the handling of incidents and notifying appropriate individuals. Escalated issues are treated with higher urgency and often shared with a wider audience.

Alert escalation is facilitated by an internal escalation tool or manual escalation based on Google-wide and team-specific escalation criteria. Production monitoring tools are integrated with the alert manager tool and communicate with the escalation tool via email and notification to on-call via pager. The escalation time and contacts are defined in the escalation tool configuration files. This leads to automated escalation if the tool does not receive an acknowledgement from the notified contacts.

Incident Resolution

After gathering the necessary information about the incident, the incident ticket is assigned to the appropriate support area based on the nature of the problem and/or the root cause. Incidents are usually forwarded to one of the corresponding technical departments:

- System Reliability Engineers / Software Engineers
- Networks
- Database Administration
- System Administration
- Application Administration
- Facilities
- Network Security
- Platform Support
- Legal Team

bernard@botmaker.io

The incident ticket is closed upon resolution of the incident. Google also has an established postmortem process for performing technical analysis of incidents after the fact to identify root cause issues, document lessons learned, and implement fixes to strengthen and improve security controls, and to prevent future incidents. Processes for notifying customers of data security and privacy incidents that affect their accounts in accordance with disclosure laws or contractual agreements are established and implemented.

Data Retention and Deletion

Google has procedures in place to dispose of confidential and need-to-know information according to the Google data retention and deletion policy and monitor for resolution of policy violations. Additionally, Google maintains defined terms regarding the return, transfer, and disposal of user data and makes these terms available to customers.

Storage Media Security

Integrity checks are in place at the application level and file system level to help ensure data integrity. At the application level, checksum comparison is performed to protect against upload

corruptions. File system consistency checks are also deployed at the storage layer using user-level programs which verify the integrity of the data. At the machine level, an integrity check system is used to synchronize system files on the root partition of production machines with a standard base image.

Google utilizes barcodes and asset tags to track the status and location of data center equipment from acquisition to installation, retirement, and destruction. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies such as Full Disk Encryption (FDE) and drive locking, to protect data at rest. Personally Identifiable Information (PII) on removable media leaving Google facilities is approved and encrypted.

When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi-stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

Redundant Architecture

Google Cloud Platform runs in a multi-tenant, geographically distributed environment on synchronized internal system atomic clocks and global positioning systems (GPS) to support the availability of services through the use of redundant architecture. Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For Google Cloud Platform, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Customer data is then stored in large, distributed databases, built on top of this file system.

The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Google uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

Disaster Recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, Google designs its infrastructure and services to be resilient to failures of software, hardware, or facilities. Redundant architecture and resources are distributed across at least two (2) geographically dispersed data centers to support the availability of services. Network connections between the data centers help ensure swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage and system administration.

Google’s Disaster Recovery program enables continuous and automated disaster readiness, response, and recovery of Google’s business, systems, and data. Google conducts disaster recovery testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, failover scenarios, operational transition, and other emergency responses. Teams that participate in the disaster recovery exercise develop testing plans and post-mortems which document the results and lessons learned from the tests.

Additionally, business continuity plans defining how personnel should respond to disruptions are made available internally and maintained. Disaster resiliency testing which covers reliability, survivability, and recovery is also conducted on an ongoing basis, and at least annually.

F. Monitoring

Functional areas across the organization are accountable for designing, implementing and operating controls to reduce risk across the organization, and engage with management for assessing controls. Management performs periodic assessments of the control environment for specific areas, such as identity management, source code management and authentication infrastructure controls. Google plans and coordinates system security and privacy-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users. Independent Internal Audit teams also perform regular audits over these areas of the control environment and the reports associated with the audits are made available to the audit committee and stakeholders. In addition, monitoring activities have been described below to communicate how monitoring is performed for Google Cloud Platform.

Leonard@bumaron.ro

Security Monitoring

Google has implemented monitoring tools to detect and report security events. Antivirus, phishing detection, and antimalware/antispam tools are also in place to protect Google's information assets. Google also maintains security event logs for privileged access, access to user data, authorized access attempts, and unauthorized access attempts. Logical access to security event logs is restricted to authorized personnel. Security event logs are monitored continuously using a Google proprietary Security Information and Event Management (SIEM) system to detect intrusion attempts and other security related events. The SIEM system is supplemented with codified logic which creates the “hunts” that trigger automated alerts to security personnel. The security alerts are generated for further investigation (manual and automated hunts) based on predefined thresholds. When a vulnerability has been identified, the Security team determines the appropriate response and tracks the issue through resolution. The owners of the affected component(s) determine the appropriate response, based on the severity and defined response criteria of the vulnerability.

Availability Monitoring

Resource management procedures are also established to monitor, maintain, and evaluate capacity demand. Google uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource

availability across their data centers and to validate that data has been replicated to more than one location.

Confidentiality Monitoring

Google has established incident response processes to report and handle events related to confidentiality as described under Incident Management above.

Privacy Monitoring

As described above, Google restricts and monitors access to customer data to only those with a valid business purpose, and further restricts the processing of customer data to authorized individuals. Google has an incident monitoring and response program designed to alert and take action if unauthorized access is discovered. New products and services are reviewed prior to launch to help ensure customer data use is in accordance with the Data Processing Addendum.

G. User Entity Responsibilities

Cloud security is a shared responsibility between a cloud service provider and its customers. Google Cloud Platform controls were designed with the assumption that certain controls should be implemented by user entities (or “customers”). These controls are known as user entity responsibilities.

This section describes additional controls that customers should consider implementing to complement the controls of the Google Cloud Platform. The list of customer control considerations presented below do not represent a comprehensive set of all the controls that should be employed by customers. Customers may be required to implement additional administrative or technical controls to meet their business and legal needs.:

User Entity Responsibilities	Trust Services Criteria
Customers are responsible for assigning responsibilities for the operation and monitoring of the Google Cloud Platform System.	Common Criteria 1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Cloud Platform System.	Common Criteria 1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
Customers are responsible for providing the appropriate training to end-users on proper use of the Google Cloud Platform System consistent with the Acceptable Use Policies and Terms of Service. Acceptable Use	Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Google Confidental Information

User Entity Responsibilities	Trust Services Criteria
Policies available at (or such URL as Google may provide): • Google Cloud Platform: https://cloud.google.com/terms/aup • Chronicle (Security Product) and Threat Intelligence for Chronicle: https://chronicle.security/legal/service-terms/ https://chronicle.security/legal/acceptable-use-policy/	
Customers are responsible for ensuring that end-users are trained on the organizational policies and procedures relevant to the use of the Google Cloud Platform System.	Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
Customers should train administrators and end-users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of the Google Cloud Platform System.	Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
Customers are responsible for training users on the use and disclosure of passwords used to authenticate to the Google Cloud Platform System.	Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Cloud Platform System.	Common Criteria 1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
	Common Criteria 5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
Customers are responsible for defining, documenting, and making available to users procedures for the operation of their instance of the Google Cloud Platform System.	Common Criteria 2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

ernald@hotmail.com

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
Customers should contact Google if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account, compromise of data, and security events.	Common Criteria 2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.
	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
Customers are responsible for ensuring any application software which they deploy onto the Google Cloud Platform System follows their specific software change management policies and procedures.	Common Criteria 4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

bernard@botmaker.io

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for periodically reviewing the configuration of the Google Cloud Platform System to help ensure it is consistent with their policies and procedures.	Common Criteria 4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for establishing organizational policies and procedures for the use or integration of third-party services.	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
Customers are responsible for reviewing the information security policies and the security capabilities in the Google Cloud Platform System to determine their applicability and modify their internal controls as appropriate.	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
Customers are responsible for defining and maintaining policies and procedures governing the customer's administration of access to the Google Cloud Platform System.	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
Customers are responsible for establishing documented policies and procedures for the transfer and sharing of information within	Common Criteria 5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

conan@botmaker.io

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
their organization and with third-party entities.	Privacy Criteria 6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.
	Privacy Criteria 6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.
Customers are responsible for provisioning, maintaining, monitoring and disabling end users' access in accordance with their internal access management policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	Privacy Criteria 5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access

bernard@botmaker.ie

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
	is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.
Customers are responsible for provisioning service availability, user roles, and sharing permissions within the Google Cloud Platform System consistent with customer organizational policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for implementing secure log-on procedures to access the Google Cloud Platform System consistent with customer access management policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

bernard@botmkt.io

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for provisioning, maintaining, and disabling end users' access in accordance with customer access management policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for reviewing users' access rights periodically, consistent with customer organizational policies, to mitigate the risk of inappropriate access.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity,

bernard@botmaker.io

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
	user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for enabling and enforcing the use of two-step verification on privileged administrator accounts.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for establishing procedures to allocate the initial password to access the Google Cloud Platform System to end-users when Google password authentication is used.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

bernard@bottaler.fr

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for configuring GCP Marketplace permissions in Google Cloud Platform consistent with customer's internal policies (GCP Marketplace contains enterprise applications that can be added to a Google Cloud Platform).	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

bernard@bottlerei.nl

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
Customers are responsible for restricting access to and monitoring the use of Application Programming Interfaces (APIs) available in the Google Cloud Platform System.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for configuring domain settings related to integration with other systems within the customer's environment consistent with customer policies.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege

bernd@bottmann.de

Google

User Entity Responsibilities	Trust Services Criteria
	and segregation of duties, to meet the entity's objectives.
Customers are responsible for ensuring that user data is exported and deleted from the Google Cloud Platform System before or within a reasonable amount of time after termination.	Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Customers are responsible for ensuring appropriate physical security controls over all devices that access the Google Cloud Platform System.	Common Criteria 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	Common Criteria 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

bernard@bottler.nl

Google Confidental Information

User Entity Responsibilities	Trust Services Criteria
Customers are responsible for ensuring any devices that access the Google Cloud Platform System or contain customer data are properly handled, secured, and transported as defined by the products requirements.	Common Criteria 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	Common Criteria 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
Customers are responsible for configuring the Google Cloud Platform System mobile device options consistent with customer policies and procedures.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
Customers are responsible for configuring data storage locations that support their business and operational resiliency requirements.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
Customers are responsible for enabling logging and monitoring functionalities to detect administrator activity, customer support activity, security events, system errors, and data deletions to support customer incident management processes.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

r.rinard@bottomline.io

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
	Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Cloud Platform System.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Privacy Criteria 7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.
Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Cloud Platform System.	Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Privacy Criteria 7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.
Customers are responsible for the deployment, configuration and modification of default security settings for cloud products including virtual machines in accordance with their information security requirements.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for ensuring that individuals creating and/or updating profiles or changing the product configurations are authorized.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for reviewing and testing features, builds, and product releases, including Application Programming Interfaces (APIs), to evaluate their impact	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements

bernard@bolinker.com

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
prior to deploying into production environments, as applicable.	changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for configuring test and/or development environments in their instance of the Google Cloud Platform System, as applicable, and restricting access to data in these environments.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for managing and testing configurations that support their business and operational resiliency objectives, and for considering Google Cloud Platform architecture recommendations.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for training, testing, and deploying AI models that are used in AI-powered applications.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for implementing any custom code necessary for the deployment of the products, and any code in public repositories for customization of their implementations.	Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
Customers are responsible for ensuring they have business recovery and backup procedures over their non-Google managed information systems that access the Google Cloud Platform System.	Common Criteria 9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
	Common Criteria 9.2: The entity assesses and manages risks associated with vendors and business partners.
Customers are responsible for ensuring that administrators do not send unnecessary employee personal data when escalating support requests to service providers, including Google.	Confidentiality Criteria 1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
	Privacy Criteria 4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

ivan.liu@botmoxe.io

Google Confidental Information

Google

User Entity Responsibilities	Trust Services Criteria
	Privacy Criteria 5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.
Customers are responsible for providing permission or instructions to utilize their data and defining the scope of data for training or fine-tuning AI/ML models	Confidentiality Criteria 1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
	Privacy Criteria 4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.
	Privacy Criteria 5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.

bernard@botnekt.io

SECTION IV - Description of Criteria, Controls, Tests and Results of Tests

bernard@botmaker.io

Description of Criteria, Controls, Tests and Results of Tests

Testing performed and results of tests of entity level controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of Google LLC and the tests performed by EY and results are the responsibility of the service auditor.

Google centrally manages the majority of the controls from their headquarters in Mountain View, CA. However, certain physical security controls are operated at the individual data centers as listed in the system description. To help ensure controls are consistently designed and implemented across the data centers, the data center security team performs a review of each data center annually that is reviewed and approved by Google management. We perform site visits of the data centers on a rotation schedule to corroborate, through independent procedures (including observation and inspection), the controls are implemented as described within Google's review. We designed the visit schedule to ensure that each data center is visited at least once every three years and that new in-scope data centers are visited in the period they are brought into scope. Additionally, we inquired of management regarding any known control deviations identified during management's internal testing. Where any material deviations were noted, we have included the results in the procedures performed.

Control criteria and related controls for systems and applications

On the pages that follow, the applicable control criteria and the controls to achieve the criteria have been specified by, and are the responsibility of, Google LLC. The sections "Tests Performed by EY" and "Results" are the responsibility of Ernst & Young LLP.

For tests of controls requiring the use of Information Produced by the Entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), EY performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the IPE, (2) inspected the query, script, or parameters used to generate the IPE, (3) tied data between the IPE and the source, and/or (4) inspected the IPE for anomalous gaps in sequence or timing to determine the data was complete, accurate, and maintained its integrity. Furthermore, in addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings); we inspect management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

bernard@bernardkoch.co

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
1. Personnel of the organization are required to acknowledge the code of conduct.	CC1.1	Inquired of the Program Manager and determined employees and extended workforce personnel were required to acknowledge the Code of Conduct as part of the terms and conditions of employment.	No deviations noted.
		Inspected internal documentation and determined employees and extended workforce personnel were required to acknowledge the Code of Conduct as part of the terms and conditions of employment.	No deviations noted.
		Inspected a sample of newly hired employees and extended workforce personnel and determined the Code of Conduct was acknowledged as part of the terms and conditions of their employment.	Deviation noted. For one (1) of twenty-five (25) sampled employees, we determined that the code of conduct was not signed timely.

bernardo@thinker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Management's Response: Management acknowledges and accepts the audit finding regarding the code of conduct not being signed within 5 weeks from the start date for one (1) sample employee out of twenty-five (25). Management noted that the code of conduct was acknowledged by the impacted sampled employee after 8 weeks of the start date (November 18, 2024) noting that the root cause of the delay on signing of the code of conduct was because the initiation of the Code of Conduct task was dependent on the employee's completion of the required onboarding steps as part of the onboarding checklist. Management reviewed the impacted employee's onboarding checklist and determined that the employee completed the required onboarding steps except for the tax withholding submission on November 18, 2024. The tax withholding submission step was completed by the employee on December 9, 2024, which then triggered the Code of Conduct task that was subsequently completed on January 3, 2025. Additionally, the required onboarding steps were appropriately tracked within the checklist and that the employee's hiring manager was appropriately informed of the series of events from the start of the employee's onboarding process up to its completion. As a result of the designed onboarding process dependencies, management determined the delay was due to an upstream process step and was not due to the failure of the control governing Code of Conduct acknowledgment once initiated.	
2. Background checks are performed on new hires as permitted by local laws.	CC1.1, CC1.4	Inquired of the Program Manager and determined background checks were performed for new hires as permitted by local laws.	No deviations noted.
		Inspected internal guidelines and determined background checks were part of the hiring process.	No deviations noted.

bernardsantmarie.com

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of new hires and determined background checks were performed as permitted by local laws.	No deviations noted.
3. The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.	CC1.1, CC1.4, CC2.2	Inquired of the Program Manager and determined privacy and information security training program was in place and relevant personnel were required to complete this training annually.	No deviations noted.
		Inspected internal documentation and determined privacy and information security training program was in place and relevant personnel were required to complete the training annually.	No deviations noted.
		Inspected a sample email notification sent to Google personnel and determined reminders were sent to complete the privacy and information security training within a specified time.	No deviations noted.
		Inspected the completion rate for the privacy and information security training for Google personnel and determined relevant personnel completed the trainings in the last 12 months or were actively being monitored until completion of training.	No deviations noted.
		Inspected the privacy and information security training material and determined that Google has outlined the importance of information security and maintaining user, customer and employee privacy.	No deviations noted.

bernard@prompt.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the continuing education documents and determined that the entity provided training programs to help ensure skill sets and technical competencies of existing employees and contractors were developed and maintained.	No deviations noted.
		Inspected the training activity dashboard and determined that the privacy and information security training was mandatory and required to be completed annually.	No deviations noted.
4. The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	CC1.1, CC1.5	Inquired of the Program Manager and determined the organization established a disciplinary process to address non-compliance with company policies, code of conduct, or other personnel requirements.	No deviations noted.
		Inspected internal documentation and determined the organization established a disciplinary process for non-compliance with the company policies, code of conduct, or other personnel requirements which could result in dismissal, lawsuits and/or criminal prosecution.	No deviations noted.
		Inspected the disciplinary procedures undertaken for sample incidents and determined appropriate action was taken in cases of non-compliance with company policies, code of conduct, or other personnel requirements.	No deviations noted.

bernardgbotmaker.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
5. The organization has established a code of conduct that is reviewed and updated as needed.	CC1.1, CC9.2, C1.1	Inquired of the Program Manager and determined the organization established a code of conduct that was reviewed and updated as needed.	No deviations noted.
		Inspected applicable policies and guidelines and determined the privacy and information security procedures as well as the code of conduct were in place and reviewed and updated as needed.	No deviations noted.
6. All board of directors exercise independent judgment. The independent / non-employee board of directors also demonstrate independence from management in exercising oversight of the development and performance of internal control.	CC1.2, CC1.5	Inquired of the Program Manager and determined the board of directors demonstrated independence from management and had established an audit and compliance committee to exercise oversight of the development and performance of internal control.	No deviations noted.
		Inspected the Alphabet proxy statement and determined that the board of directors, including the members of the audit and compliance committee, demonstrated independence from management.	No deviations noted.
		Inspected the Alphabet proxy statement and determined the board of directors had relevant expertise and exercised oversight over controls and performance of internal control.	No deviations noted.

bernard@ormaze.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of quarterly audit and compliance committee minutes of meeting and determined the committee met on a quarterly basis and relevant information resulting from internal and external assessments over internal control were communicated to the board of directors.	No deviations noted.
7. The organization has implemented a formal reporting structure that is made available to personnel.	CC1.3, CC1.4	Inquired of the Program Manager and determined the organization implemented a formal reporting structure that was made available to personnel.	No deviations noted.
		Inspected the organization's intranet and determined organizational charts showing formal reporting structure were made accessible to employees and included drill-down functionality to identify employees within the organizational structure, including employees in their functional teams.	No deviations noted.
		Inspected a sample communication and determined top level management changes were communicated internally and externally.	No deviations noted.
		Inspected the meeting minutes of a sample Board of Directors forum and determined management considered requirements such as integrity and security when defining authorities, structures, reporting lines, and responsibilities.	No deviations noted.

bernard@bottrakers.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected procedural documents and determined management planned and prepared for succession by developing contingency plans for assignments of responsibility.	No deviations noted.
8. New hires or internal transfers are required to go through an official recruiting process during which they are screened against detailed job descriptions and interviewed to assess competence.	CC1.3, CC1.4	Inquired of the Program Manager and determined that new hires and internal transfers were required to go through an official recruiting process during which their qualifications and experience were screened against detailed job descriptions to help ensure that they were competent to fulfill their responsibilities.	No deviations noted.
		Inspected relevant internal hiring guidelines and determined that the organization has implemented an official recruiting process for new hires and internal transfers.	No deviations noted.
		Inspected a sample of new hires and internal transfers and determined positions had detailed job description including minimum and preferred qualifications, such as requisite skills and experiences, which candidates must meet in order to be hired.	No deviations noted.
		Inspected a sample of new hires and internal transfers and determined they went through a formal recruiting process and were screened against detailed job descriptions and interviewed to assess competence.	No deviations noted.

bernard@bathmaster.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
9. Company goals and responsibilities are required to be developed and communicated by management on a periodic basis, and amended as needed. Results are evaluated and communicated to employees.	CC1.3, CC1.5, CC2.2, CC3.1	Inquired of the Program Manager and determined company goals and responsibilities were developed and communicated by management and amended as needed. Results of the annual goals were evaluated and communicated to employees.	No deviations noted.
		Inspected a sample of annual objectives and key results and determined company goals and responsibilities were developed and communicated by management.	No deviations noted.
		Inspected a sample announcement and determined results of previous goals were communicated to employees.	No deviations noted.
10. Information security is managed by an executive who is dedicated to Security, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.	CC1.5	Inquired of the Program Manager and determined information security and privacy was managed by an executive who is dedicated to security and privacy, is independent of information technology responsibility, and may escalate matters and issues concerning security and privacy to the board level.	No deviations noted.
		Inspected the security organizational structure and determined an executive was dedicated to security and privacy, who was independent of information technology responsibilities.	No deviations noted.

bernardshotmarket.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the meeting minutes and determined the Security and Privacy team met with relevant personnel to discuss security and privacy issues, and escalated security and privacy concerns to the board of directors, as necessary.	No deviations noted.
11. The organization periodically reviews and validates the design, operation and control record of in-scope compliance controls.	CC1.5, CC4.1, CC4.2	Inquired of the Program Managers and Internal Audit and determined that the organization had an established internal compliance function which periodically evaluates, reviews and validates the design, operation and management's compliance with security and privacy controls.	No deviations noted.
		Inspected evaluations performed by the internal compliance function for a sample of semiannual periods and determined that the compliance function performed an evaluation of management's compliance with security and privacy controls.	No deviations noted.
		Inspected evaluations performed by management for a sample of quarters and determined that management performed an evaluation of their compliance with security and privacy controls.	No deviations noted.
		Inspected the meeting invites related to the organization's annual organizational risk assessment and determined that the company's operational objectives, and potential impacts and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.

bernard@attacker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
12. Teams within the organization document standard operating procedures and make them available to authorized personnel	CC2.1	Inquired of the Program Manager and determined that teams within the organization document standard operating procedures and make them available to authorized personnel.	No deviations noted.
		Inspected internal team handbooks for a sample Google Cloud Platform product team and determined that documented standard operating procedures were in place and available to authorized personnel.	No deviations noted.
13. The organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	CC2.1, CC2.2	Inquired of the Program Manager and determined the organization established security policies and procedures, which clearly defined information security responsibilities for all employees, including the Information Security team. The organization managed operational risk by delegating decisions on risk identification and resource prioritization.	No deviations noted.
		Inspected relevant security policies and procedures and determined they defined information security responsibilities of employees and the Information Security Team.	No deviations noted.
		Inspected the organization's risk assessment and determined the organization managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of the organization's products and services.	No deviations noted.

bernardoquatrin@gmail.com

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
14. The organization has established a process to review and approve requests for policy exceptions.	CC2.1, CC2.2	Inquired of the Program Manager and determined Google has a policy exception process to ensure a formal approval and risk evaluation are performed.	No deviations noted.
		Inspected applicable policies and determined the process to request and process policy exceptions was documented.	No deviations noted.
		Inspected a sample of policy exceptions and determined they followed the process as described in the policy.	No deviations noted.
15. System changes are reviewed and approved by a separate technical resource before moving into production.	CC2.1, CC8.1	Inquired of the Program Manager and determined system changes were reviewed and approved by a separate technical resource before migration to production.	No deviations noted.
		Inspected the applicable code for the organization's code management system and determined system changes required a review by a separate technical resource before migration to production.	No deviations noted.
		Inspected evidence of transaction testing made by a user to the version code management system and determined that it required changes to be reviewed by a separate technical resource before migration to production.	No deviations noted.

bernard@bountaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
16. The descriptions of the organization's systems (including their scope and boundaries) are made available to internal teams.	CC2.2	Inquired of the Program Manager and determined that descriptions of the organization's systems, including their scope and boundaries, were made available to internal teams.	No deviations noted.
		Inspected the internal website for all internal products and determined descriptions of the organization's systems and their boundaries were available to the organization's internal product teams.	No deviations noted.
		Inspected the internal product website and determined a description of the organization's system and its boundaries were available to the organization's internal product teams.	No deviations noted.
17. Changes to customer facing services that may affect confidentiality, processing integrity and / or availability are communicated to relevant personnel and impacted customers.	CC2.2, CC2.3	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.
		Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
		Inspected a sample product launch and determined a design document and privacy review were completed prior to the launch.	No deviations noted.

bernardoquintero.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of official product blogs for product and feature releases and determined relevant personnel and impacted customers were notified.	No deviations noted.
18. Customer responsibilities are described on the organization's product websites or in system documentation.	CC2.2, CC2.3	Inquired of the Program Manager and determined customer responsibilities were described on product websites or in system documentation.	No deviations noted.
		Inspected the GCP website or in system documentation accessible by external customers and determined customer responsibilities were described.	No deviations noted.
19. The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	CC2.2, CC5.3	Inquired of the Program Manager and determined the organization had security policies addressing confidentiality, integrity, and availability that were approved by management and published on the intranet which is accessible to employees.	No deviations noted.
		Inspected internal documentation and determined security policies addressing confidentiality, integrity and availability have been approved by management.	No deviations noted.
		Inspected internal documentation and determined the organization has security policies addressing confidentiality, integrity and availability communicated and published on the intranet and accessible to employees.	No deviations noted.

bernard@barnard.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
20. The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	CC2.2, CC7.3	Inquired of the Program Manager and determined the organization had an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No deviations noted.
		Inspected the organization's incident response policy and determined policies and procedures were in place which outline a quick, effective, and orderly response to information security incidents. In addition, classification, prioritization, and escalation of security incidents per criticality are also identified and mechanisms are defined to measure and monitor the type and scope of security incidents.	No deviations noted.
		Inspected internal documentation and determined the organization maintained and periodically updated the incident response policy.	No deviations noted.
21. Descriptions of the organization's system and its boundaries are available to external parties via ongoing communications with customers or via its official blog postings.	CC2.3	Inquired of the Program Manager and determined descriptions of the organization's system and its boundaries were available to authorized external users via ongoing communications with customers or via its official blog postings.	No deviations noted.
		Inspected the organization's official blog postings and determined descriptions of the organization's system and its boundaries were communicated.	No deviations noted.

bernardo@attacker.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
22. The organization provides external users with mechanisms to report security issues, incidents and concerns.	CC2.3	Inquired of the Program Manager and determined that the organization provides external users with mechanisms to report security issues, incidents, and concerns.	No deviations noted.
		Inspected the organization's websites and determined mechanisms were available for external users to report security issues, incidents, and concerns.	No deviations noted.
		Inspected the organization's websites and determined separate communication channels were in place to enable anonymous or confidential communication when normal channels were inoperative or ineffective.	No deviations noted.
		Inspected a sample incident ticket raised by an external user through the established mechanisms to validate that the issue or concern was received by the organization.	No deviations noted.
23. The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	CC2.3	Inquired of the Program Manager and determined Google published its commitments to security, availability, processing integrity and confidentiality to external users via Terms of Service (ToS).	No deviations noted.
		Inspected Google Cloud Platform's Terms of Service and product websites and determined Google's commitments to security, availability, processing integrity, and confidentiality are published for external users.	No deviations noted.

bernard@protonmail.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
24. The organization notifies customers of updates to its confidentiality guidelines, objectives, and practices.	CC2.3, C1.1	Inquired of the Program Manager and determined the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.
		Inspected the organization's Terms of Service and determined the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.
		Inspected GCP's customer documentation and determined that the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.
25. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by management.	CC3.1, CC3.2, CC3.3, CC3.4	Inquired of the Program Manager and determined the organization conducted periodic information security risk assessments to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No deviations noted.
		Inspected applicable documentation and determined a risk management framework was developed and documented to manage risk to an acceptable level and defined resolution time frames for risks.	No deviations noted.

kenard@ctmgr.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the risk assessment and determined the organization conducted periodic information security risk assessments and identified, evaluated and mitigated risks to acceptable levels based on risk criteria, which are established, documented and approved by management.	No deviations noted.
		Inspected the organization's risk assessment and determined management signed off on the annual risk assessments performed.	No deviations noted.
26. The organization develops and maintains a risk management framework to manage risk to an acceptable level.	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2	Inquired of the Program Manager and determined the organization developed and maintained a risk management framework to manage risk to an acceptable level.	No deviations noted.
		Inspected the vulnerability management and severity guidelines and determined a risk management framework was developed and documented to manage risk to an acceptable level, defined resolution time frames for risks, and to consider the potential for fraud.	No deviations noted.
		Inspected internal documentation and determined the organization maintains a security risk assessment framework to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented and signed off by management.	No deviations noted.

bernardshortmaker.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the organization's risk assessment and determined the organization evaluates qualitative and quantitative factors to identify residual risk in order to manage risk to an acceptable level.	No deviations noted.
		Inspected meeting invites and relevant documentation from the organization's annual risk assessment discussion and determined the organization's operational objectives, potential impacts, and changes to the business model were considered.	No deviations noted.
		Inspected the internal insider risk site and determined the organization considered insider risk in its risk management framework to manage risk to an acceptable level.	No deviations noted.
27. The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, CC7.2, A1.3	Inquired of the Program Manager and determined the organization conducted periodic information security risk assessments to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No deviations noted.
		Inspected applicable documentation and determined a risk management framework was developed and documented to manage risk to an acceptable level and defined resolution time frames for risks.	No deviations noted.

bernard@bottomley.ie

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the risk assessment and determined the organization conducted periodic information security risk assessments and identified, evaluated and mitigated risks to acceptable levels based on risk criteria, which are established, documented and approved by management.	No deviations noted.
		Inspected the organization's risk assessment and determined management signed off on the annual risk assessments performed.	No deviations noted.
28. The organization conducts periodic privacy risk assessments to identify and evaluate risks related to the handling of user data.	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, A1.3	Inquired of the Program Manager and determined the organization conducted periodic privacy risk assessments to identify and evaluate risks related to the handling of user data.	No deviations noted.
		Inspected internal documentation and determined the organization had a formal risk assessment process that included policies and procedures for identification, evaluation, ownership, treatment, and acceptance of privacy risks.	No deviations noted.
		Inspected the risk assessment and determined the organization identified and evaluated risks related to the handling of user data periodically.	No deviations noted.
29. The organization has established a dedicated security team engaging in security and privacy of customer data and	CC3.2	Inquired of the Program Manager and determined that the organization has established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.	No deviations noted.

bernardshortreaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
managing security 24 x 7 worldwide.		Inspected relevant policies and guidelines and determined that the organization established a dedicated security team to engage in security and privacy of customer data.	No deviations noted.
		Inspected internal documentation and determined that a dedicated security team engaged in security and privacy of customer data managed security 24 x 7 worldwide.	No deviations noted.
		Inspected the on-call calendar configuration and determined that the on-call calendar was maintained according to a defined set of rules.	No deviations noted.
		Inspected the on-call calendar configuration and determined that on-call rotation schedules were automated and any change in the schedule was subject to the management's approval process.	No deviations noted.
		Inspected the Incident Response team's on-call schedule and determined that the security team engaged in security and privacy was available 24 x 7.	No deviations noted.
30. The organization has implemented a vulnerability management program to detect	CC3.2, CC3.3,	Inquired of the Program Manager and determined the organization had a vulnerability management program in place to detect and remediate system vulnerabilities.	No deviations noted.

bernard@antmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
and remediate system vulnerabilities.	CC6.8, CC7.1, CC7.2	Inspected internal policies and guidelines and determined the organization had a vulnerability management program in place to identify, detect, report, prioritize, and remediate system vulnerabilities.	No deviations noted.
		Inspected internal documentation and determined vulnerabilities were classified based on the priority level.	No deviations noted.
		Inspected relevant configurations and determined vulnerabilities were tracked through an internal ticketing system as outlined in the vulnerability management program.	No deviations noted.
		Inspected a sample of identified vulnerabilities and determined they were tracked in an internal ticketing system through remediation.	No deviations noted.
31. The organization has policies and guidelines that govern the acceptable use of information assets.	CC3.2, CC6.1	Inquired of the Program Manager and determined the organization established policies and procedures that governed the acceptable use of information assets.	No deviations noted.
		Inspected the relevant documentation and determined Google established policies and procedures that governed the acceptable use of information assets.	No deviations noted.
32. Penetration tests are performed using a defined methodology and frequency aligned with compliance	CC4.1	Inquired of the Program Manager and determined the organization performed penetration tests by qualified internal personnel or an external service provider at least annually.	No deviations noted.

bernard@dalmaker.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes		Inspected the penetration test report and related documentation and determined that identified deficiencies were assessed, prioritized, followed up and addressed based on their criticality.	No deviations noted.
		Inspected relevant documentation and determined the organization has policies and guidelines in place for penetration tests performed by qualified internal personnel or an external service provider.	No deviations noted.
		Inspected relevant documentation and determined a penetration test, which included critical infrastructure components, occurred within the past year and results were documented comprehensively.	No deviations noted.
33. The organization has an established Internal Audit function which evaluates management's compliance with security controls.	CC4.1, CC4.2, CC5.3	Inquired of the Program Managers and Internal Audit and determined that the organization had an established internal compliance function which periodically evaluates, reviews and validates the design, operation and management's compliance with security and privacy controls.	No deviations noted.
		Inspected evaluations performed by the internal compliance function and determined that the compliance function performed an evaluation of management's compliance with security and privacy controls.	No deviations noted.

bernard@thader.ie

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected evaluations performed by management for a sample of quarters and determined that management performed an evaluation of their compliance with security and privacy controls.	No deviations noted.
		Inspected the meeting invites related to Google's annual organizational risk assessment and determined that the company's operational objectives, and potential impacts and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.
34. Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	CC4.1, CC5.3	Inquired of the Program Manager and determined security and privacy policies are reviewed at least annually, and supporting standards, guidelines, and FAQs are created and updated as needed.	No deviations noted.
		Inspected internal documentation and determined that security and privacy policies, supporting standards, guidelines and FAQS were in place.	No deviations noted.
		Inspected internal documentation and determined security and privacy policies were reviewed at least annually and authorized before they were implemented.	No deviations noted.
		Inspected the most recent security and privacy policy reviews and determined policies were approved by authorized personnel or committee, reviewed at least annually, and updated as needed.	No deviations noted.

bernard@bathaker.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
35. The organization separates duties of individuals by granting users access based on job responsibilities and least privilege, and limiting access to only authorized users.	CC5.1	Inquired of the Program Manager and determined the organization separated duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	No deviations noted.
		Inspected relevant policies and guidelines, and determined the organization separates duties of individuals as necessary, by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	No deviations noted.
		Inspected the configurations within the source code management system and determined that the organization separates duties of individuals by granting users access based on job responsibilities and least privilege, and limiting access to only authorized users.	No deviations noted.
		Observed an attempt to grant user access to a group based on job responsibilities and least privilege by an appropriate approver and determined access was granted.	No deviations noted.
		Observed an attempt to grant user access to a group based on job responsibilities and least privilege without an appropriate approver and determined access was not granted.	No deviations noted.

bernard@bottomline.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample system generated log for access to production machines, support tools, and network devices and determined access approvals and modifications to the access lists were recorded.	No deviations noted.
36. The organization has an internal audit function and regularly engages independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	CC5.1, CC5.2	Inquired of the Program Manager and determined the organization had an internal audit function and regularly engaged independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	No deviations noted.
		Inspected documents related to internal audit and determined the organization had an internal audit function and regularly engaged third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security.	No deviations noted.
		Inspected a list of the organization's security compliance certifications and determined the organization regularly engaged third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security.	No deviations noted.

bernard@[illegible].ie

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the meeting invites related to the organization's annual organizational risk assessment and determined the organization's operational objectives, potential impacts, and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.
37. Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	CC5.2	Inquired of the Operations Manager and determined critical data center equipment supporting the organization's products and services were continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	No deviations noted.
		Inspected internal documentation and determined routine preventative and regular maintenance processes (including ad-hoc repairs) were communicated to data center teams according to organizational requirements.	No deviations noted.
		Inspected a sample of maintenance records for the UPS, generators, fire suppression systems, fire extinguishers, emergency lighting systems, and HVAC systems, and determined the organization performed and recorded routine preventative and regular maintenance in accordance with organizational requirements over critical data center equipment.	No deviations noted.

bernard@drinkers.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
38. The organization has established an offboarding procedure for personnel, which governs the removal of access and return of assets.	CC5.2	Inquired of the Program Manager and determined the organization had established offboarding procedures for personnel, which governed the removal of access and return of assets.	No deviations noted.
		Inspected internal guidelines and determined the organization had established offboarding procedures for personnel, which governed the removal of access and return of assets.	No deviations noted.
		Inspected internal guidelines and determined internal and external employees were informed that obligations to comply with relevant laws, regulations, and provisions regarding information security remain valid, even if the area of responsibility changes or the employment relationship is terminated.	No deviations noted.
39. The organization has guidelines specifying the security requirements for new and existing information systems.	CC5.2, CC5.3	Inquired of the Program Manager and determined the organization had an established policy specifying the security requirements for new information systems, or enhancements to existing information systems.	No deviations noted.
		Inspected internal policies and determined security requirements were specified for new information systems, or enhancements to existing information systems.	No deviations noted.

bernard@anthropic.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected publicly available documentation and determined Google outlined security requirements for new information systems, or enhancements to existing information systems related to its services.	No deviations noted.
40. Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis upon submission of a termination request by Human Resources or a manager.	CC5.2, CC6.2, CC6.3	Inquired of the Program Manager and determined access to production machines, support tools, network devices and corporate assets was automatically removed on a timely basis upon submission of a termination request by Human Resources or a manager.	No deviations noted.
		Inspected relevant documentation and determined requirements for terminating users with access to production machines, support tools, network devices and corporate assets were documented.	No deviations noted.
		Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined it was configured to remove access upon submission of a termination request by Human Resources or a manager.	No deviations noted.
		Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined that any failures in the process will generate an alert.	No deviations noted.

bernard@bothaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample alert from the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined that the failure was resolved in a timely manner.	No deviations noted.
		Inspected a sample of terminated users and determined that access to production machines, support tools, network devices, and corporate assets was automatically revoked by the automated tool within seven (7) days of the user's termination date.	No deviations noted.
41. Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	CC5.2, CC6.2, CC6.3, CC6.6	Inquired of the Program Manager and determined that access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	No deviations noted.
		Inspected relevant documentation and formal procedures for managing user access to production machines, support tools, and network devices via access control lists and determined that access requests and modifications must be recorded and approved by appropriate administrators.	No deviations noted.

bernard@baltraker.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the configurations within the source code management system and determined that the relevant access control list systems were configured to enforce approval from a group administrator prior to a user receiving access to production machines, support tools, and network devices.	No deviations noted.
		Observed an attempt to grant user access to a group with the appropriate approval from the group administrator and determined access was granted.	No deviations noted.
		Observed an attempt to grant user access to a group without the appropriate approval from the group administrator and determined access was not granted.	No deviations noted.
		Inspected a sample of system generated logs for access to production machines, support tools, and network devices and determined access approvals and modifications to the access lists were recorded.	No deviations noted.
42. The organization has policies and guidelines that govern access to information systems.	CC5.3	Inquired of the Program Manager and determined the organization established policies and procedures that govern access to information systems.	No deviations noted.
		Inspected the relevant documentation and determined Google established policies and procedures that govern access to information systems.	No deviations noted.

bernard@pottinger.ie

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
43. The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	CC5.3, CC7.5	Inquired of the Program Manager and determined change management policies, including security code reviews, were in place, and procedures for tracking, testing, approving, and validating changes were documented.	No deviations noted.
		Inspected internal policies and determined practices for security code review, tracking, testing, approving, and validating changes were documented.	No deviations noted.
44. The organization has a security guideline that requires users to lock their workstations and mobile devices when unattended. Workstations are configured to initiate a password protected screen-saver after 15 minutes of inactivity (i.e., no input from device user).	CC6.1	Inquired of the Program Manager and determined a security guideline was in place that required users to lock workstations and mobile devices when unattended.	No deviations noted.
		Inspected internal policies and determined the organization required users to lock their workstations and mobile devices when unattended.	No deviations noted.
		Inspected the idle time configurations propagated to workstations and determined they were configured to enforce password standards.	No deviations noted.
		Performed on-site inspections for a sample of offices and determined that employees followed appropriate office security practices including locking workstations when unattended.	No deviations noted.

bernard@catbaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample of corporate machines and determined users were locked out after reasonable amount of time of inactivity.	No deviations noted.
45. The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/ or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	CC6.1	Inquired of the Program Manager and determined networks were segregated based on the types of services, users and information systems. Inquired and determined that networks are physically and/or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	No deviations noted.
		Inspected internal documentation and determined networks were designed to be logically or physically segregated.	No deviations noted.
		Inspected configurations and determined networks used for migration and generation of virtual machines were physically and logically segregated from other networks.	No deviations noted.
		Inspected internal documentation and determined networks for the management of the infrastructure and for the operation of management consoles were separated.	No deviations noted.
		Inspected internal documentation and determined processes were defined to maintain separate development, testing and production environments.	No deviations noted.

bernard@bettrack.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected network diagrams and determined high-risk environments were designed to be physically and logically segregated from other networks.	No deviations noted.
46. The organization has an established key management process in place to support the organization's use of cryptographic techniques.	CC6.1	Inquired of the Program Manager and determined the organization had an established key management process in place to support the organization's internal cryptographic techniques.	No deviations noted.
		Inquired of the Program Manager and determined the organization had an established key management process in place to support the organization's external use of cryptographic techniques.	No deviations noted.
		Inspected internal documentation and determined key management procedures were in place for internal cryptographic techniques.	No deviations noted.
		Inspected internal documentation and determined key management procedures were in place for external cryptographic techniques.	No deviations noted.
		Inspected the code configuration and determined that internal certificates expired after a set duration when the certificate is issued.	No deviations noted.
		Inspected the code configuration for internal certificate revocations and determined certificate revocations conformed to the organization's policies and procedures.	No deviations noted.

bernard@tomoki.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the code configuration enforcing encryption and certificate authentication and determined internal use of cryptographic techniques conformed to the organization's policies and procedures.	No deviations noted.
		Inspected the code configuration enforcing encryption and certificate authentication and determined external use of cryptographic techniques conformed to the organization's policies and procedures.	No deviations noted.
		Inspected the code configuration for external certificate revocations and determined certificate revocations used proper authorizations and changes to the list of certificate revocations were restricted.	No deviations noted.
		Observed an engineer attempt to request a certificate and determined the key management process was followed to support the organization's internal use of cryptographic techniques.	No deviations noted.
		Inspected a sample of internal certificate revocation requests and determined certificates were revoked timely.	No deviations noted.
		Observed an engineer attempt to request a certificate and determined the key management process was followed to support the organization's external use of cryptographic techniques.	No deviations noted.

bernard@lighthaler.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of external certificate revocation requests and determined certificates were revoked timely.	No deviations noted.
47. Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.	CC6.1	Inquired of the Program Manager and determined access to network devices was authenticated via user ID, password, security key, and/or certificate.	No deviations noted.
		Inspected the access configuration for production network devices and determined it required authentication via user ID, password, security key, and/or certificate.	No deviations noted.
		Observed a user attempt to obtain access to network devices after authenticating via user ID, password, security key, and/or certificate and determined that the user successfully obtained access.	No deviations noted.
		Observed a user attempt to obtain access to network devices without first authenticating via user ID, password, security key, and/or certificate and determined that the user failed to obtain access.	No deviations noted.
48. The organization has established formal guidelines for passwords to govern the	CC6.1	Inquired of the Program Manager and determined the organization had established password guidelines to govern the management and use of authentication mechanisms.	No deviations noted.

bernard@tarnaki.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
management and use of authentication mechanisms.		Inspected relevant documentation and determined formal guidelines for passwords were established to govern the management and use of authentication mechanisms.	No deviations noted.
		Inspected the relevant configurations and determined passwords were transmitted and stored in an encrypted manner.	No deviations noted.
		Inspected the password configurations propagated to servers and determined they were configured to enforce password requirements.	No deviations noted.
		Observed user attempt to login using incorrect password and determined the account was locked out after exceeding the maximum number of attempts allowed.	No deviations noted.
49. The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege.	CC6.1	Inquired of the Program Manager and determined the organization had an established policy to ensure access to information resources, including data and the systems which store or process data, was authorized based on the principle of least privilege.	No deviations noted.
		Inspected internal policies and determined the organization had an established policy to ensure access to information resources, including data and the systems which store or process data, was authorized based on the principle of least privilege.	No deviations noted.

bernard@pathmaker.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
50. External system users are identified and authenticated via the Google Accounts or the BYOID authentication system before access is granted.	CC6.1	Inquired of the Program Manager and determined external system users were identified and authenticated via the organization's authentication system before access is granted.	No deviations noted.
		Inspected the configuration supporting the login functionality and determined users were identified and authenticated via the organization's authentication system before access was granted.	No deviations noted.
		Observed an external system user login with a valid organizational account and determined access was granted.	No deviations noted.
		Observed an external system user attempt to login with an invalid organizational account and determined access was denied.	No deviations noted.
51. Customer data that is uploaded or created is encrypted at rest.	CC6.1	Inquired of the Program Manager and determined customer data that was uploaded or created was encrypted at rest.	No deviations noted.
		Inspected the policies surrounding customer data encryption at Google and determined guidelines and policies were implemented to protect customer data.	No deviations noted.
		Inspected the encryption configuration for storage devices with customer data at rest and determined that encryption was enabled to protect customer data.	No deviations noted.

bernard@cotinga.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of storage devices with customer data and determined they displayed an encrypted state.	No deviations noted.
52. The organization has established mechanisms governing the configuration and security of corporate-managed CrOS, Android and iOS devices providing privileged access.	CC6.1	Inquired of the Program Manager and determined the organization has established mechanisms governing the configuration and security of corporate-managed devices providing privileged access.	No deviations noted.
		Inspected relevant documentation and determined that policies are in place to govern the device management, security, and baseline requirements of corporate-managed mobile devices providing privileged access.	No deviations noted.
		Inspected relevant documentation and determined that policies are in place to govern the use of encryption for corporate-managed mobile devices providing privileged access.	No deviations noted.
		Inspected relevant documentation and determined policies are in place for access protection and identity management for corporate-managed mobile devices.	No deviations noted.
		Inspected relevant policies and documentation and determined unofficial operating systems are prohibited on corporate-managed mobile devices.	No deviations noted.
		Inspected relevant policies and documentation and determined requirements for BYOD mobile devices for use in the corporate environment are established.	No deviations noted.

bernard@...

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the configuration for corporate-managed devices with privileged access and determined the organization implemented access protection, identity, and authorization management protections.	No deviations noted.
		Inspected the device settings on a corporate-managed device with privileged access and determined access protection, identity, and authorization management protections are implemented as configured.	No deviations noted.
		Inspected a sample device to determine that technical measures are in place to allow remote deletion of company data on managed endpoint devices.	No deviations noted.
53. Wireless connections to Corporate resources at facilities managed by the organization are encrypted	CC6.1	Inquired of the Program Manager and determined wireless connections to corporate resources at the organization's facilities were encrypted.	No deviations noted.
		Inspected internal documentation and determined wireless connections to corporate resources at the organization's facilities were encrypted.	No deviations noted.
		Inspected a remote wireless connection to corporate resources and determined that remote access to the corporate network was encrypted.	No deviations noted.
54. Security event logs are protected and access is restricted to authorized personnel.	CC6.1, CC6.2	Inquired of the Program Manager and determined security event logs were protected and access was restricted to authorized personnel.	No deviations noted.

bernard@lothlorien.ie

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected internal documentation and determined policies and procedures for restriction of logical access to audit logs to authorized personnel were in place.	No deviations noted.
		Inspected the system code related to audit logs and determined log files are frozen and access to modify logs is restricted	No deviations noted.
		Inspected a sample of members with access to audit logs and determined they were appropriate to have access to audit logs.	No deviations noted.
		Inspected a sample semiannual user access review and determined access to audit logs was reviewed on a periodic basis and that appropriate action was taken to resolve inappropriate access, if applicable.	No deviations noted.
55. Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.	CC6.1, CC6.2	Inquired of the Program Manager and determined access to the corporate network, which further provides access to production machines, network devices, and support tools, required a unique ID, password, valid credentials, and/or machine certificates.	No deviations noted.
		Inspected the configuration for access to corporate network, network devices, production machines, and support tools and determined a unique ID, password, valid credentials, and/or machine certificates were required.	No deviations noted.

kurnard@bonnaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a user attempt to create a user with a username belonging to another user and determined that a duplicate username could not be assigned.	No deviations noted.
		Observed a user attempt to create, delete, and recreate an account with the same username and determined the accounts were assigned unique IDs.	No deviations noted.
		Observed a user attempt to access the corporate network without valid credentials and determined access was denied.	No deviations noted.
		Observed a user attempt to access the corporate network with valid credentials and determined access was granted.	No deviations noted.
		Observed a user attempt to access the production machines with an authorized private key by using a valid SSH certificate and determined access was allowed.	No deviations noted.
		Observed a user attempt to access the production machines without an authorized private key by using an invalid SSH certificate and determined access was denied.	No deviations noted.
		Observed a user attempt to obtain access to network devices after authenticating via user ID, password, security key, and/or certificate and determined that the user successfully obtained access.	No deviations noted.

bernard@bernard.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a user attempt to obtain access to network devices without first authenticating via user ID, password, security key, and/or certificate and determined that the user failed to obtain access.	No deviations noted.
		Observed a user attempt to access an internal support tool with valid credentials and determined access was granted.	No deviations noted.
		Observed a user attempt to access an internal support tool without valid credentials and determined access was not granted.	No deviations noted.
		Observed an engineer attempt to request a certificate and determined the key management process was followed to support the organization's internal and external use of cryptographic techniques.	No deviations noted.
		Inspected a sample of internal and external certificate revocation requests and determined certificates were revoked timely.	No deviations noted.
56. Mechanisms are in place to detect attempts, and prevent connections to the organization's network by unauthorized devices.	CC6.1, CC6.2	Inquired of the Program Manager and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.

bernard@[illegible]

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected relevant documentation and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
		Inspected relevant configurations and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
		Observed a user with an authorized device attempt to connect to the organization's network and determined the connection was successful.	No deviations noted.
		Observed an unauthorized user attempt to connect to the organization's network and determined access was denied.	No deviations noted.
		Observed a user attempt to connect to the production network with a valid certificate and determined the connection was successful.	No deviations noted.
		Observed a user attempt to connect to the production network without a valid certificate and determined that access was denied.	No deviations noted.
		Observed a user modify their certificate and determined that access was disconnected.	No deviations noted.

bernard@bothsides.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample alert and determined mechanisms were in place to detect attempts at unauthorized connections to the organization's network.	No deviations noted.
57. Personnel access to internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	CC6.1, CC6.6	Inquired of the Program Manager and determined access to sensitive systems and applications requires two-factor authentication in the form of user ID, password, security key, and/or certificate.	No deviations noted.
		Inspected the applicable policy and determined access to sensitive systems and applications required two-factor authentication in the form of user ID, password, security key and/or certificate.	No deviations noted.
		Inspected relevant policy documentation and determined the organization has an established policy that specifies the use of emergency credentials.	No deviations noted.
		Inspected the configuration and determined that personnel access to sensitive internal systems and applications required two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	No deviations noted.
		Observed a user attempt to gain access to a production machine with a valid user ID, password, security key, and certificate and determined access was granted.	No deviations noted.

bernard@shamoo.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a user attempt to gain access to a production machine without a valid certificate and determined access was not granted.	No deviations noted.
		Observed a user attempt to gain access to a production machine with valid emergency access credentials and determined access was granted.	No deviations noted.
		Observed a user attempt to gain access to a production machine without valid emergency access credentials and determined access was not granted.	No deviations noted.
58. Remote access to corporate machines requires a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate.	CC6.1, CC6.6	Inquired of the Program Manager and determined remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate.	No deviations noted.
		Inspected relevant documentation and determined remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificates.	No deviations noted.
		Inspected the remote access configuration and determined it required a Company issued digital certificate to be installed on the connecting device.	No deviations noted.

bernard@bernard.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the authentication settings for remote access to corporate machines and determined two-factor authentication was required.	No deviations noted.
		Observed a user attempt to gain remote access to corporate machine with a device that had a Company issued digital certificate installed and two-factor authentication and determined remote access to the corporate environment was successful.	No deviations noted.
		Observed a user attempt to gain remote access to corporate machine with a device that did not have a Company issued digital certificate installed and determined remote access to the corporate environment was denied.	No deviations noted.
		Observed a user attempt to gain remote access to corporate machine with a device without two-factor authentication and determined remote access to the corporate environment was denied.	No deviations noted.
59. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	CC6.1, CC6.6, CC6.7	Inquired of the Program Manager and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
		Inspected internal policies regarding encryption mechanisms and determined the organization used encryption to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.

bernardo@othor.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected externally available documentation and determined the organization communicated how user authentication and administrator sessions transmitted over the Internet were encrypted.	No deviations noted.
		Inspected encryption mechanism documentation and configurations, and determined user authentication and administrator sessions transmitted over the Internet were encrypted.	No deviations noted.
		Observed connection settings to the organization's external websites for a user and an administrator and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
		Inspected the server scan results and determined the organization used encryption mechanisms to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
60. The organization has established guidelines for protecting against the risks of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems.	CC6.1, CC6.7	Inquired of the Program Manager and determined the organization has established guidelines for protecting against the risk of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems. The organization also requires two-factor authentication and valid certificates to be installed on the connecting device.	No deviations noted.

bernard@ey.com

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected relevant documentation and determined guidelines and policies were implemented to protect information accessed and govern the use of system encryption for communication.	No deviations noted.
		Inspected authentication settings for production and remote access and determined access to the system required two-factor authentication and valid certificates to be installed on the connecting device.	No deviations noted.
		Inspected connection settings for a user connecting to the organization network and determined that encryption mechanisms were used.	No deviations noted.
		Observed a user attempt to gain access to the environment with a device that had Company issued digital certificates installed and determined access was successful.	No deviations noted.
		Observed a user attempt to gain access to the environment with a device that did not have Company issued digital certificates installed and determined access was denied.	No deviations noted.
61. The organization uses a version control system, to manage source code, documentation, release labeling, and other	CC6.1, CC8.1	Inquired of the Program Manager and determined the organization used an internal code management system to manage source code, documentation, release labeling, and that access to the system has to be approved.	No deviations noted.

bernard@ernaer.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
functions. Access to the system must be approved.		Inspected internal documentation and determined the organization uses a version control system, to manage source code, documentation, release labeling, and other functions.	No deviations noted.
		Inspected code change management tools and determined that there was a version control system in place to manage source code, code documentation, and release labeling.	No deviations noted.
		Inspected the system configurations for the code management system and determined the system was configured to require an approval prior to granting access to the version control system.	No deviations noted.
62. The organization has a published policy about retention and deletion of user data.	CC6.1, C1.1, C1.2, P4.2, P4.3	Inquired of the Program Manager and determined Google has a User Data Retention and Deletion Policy.	No deviations noted.
		Inspected the User Data Wipeout Policy and other related documentation, and determined they established guidelines to govern the retention and deletion of user data.	No deviations noted.
63. The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the	CC6.1, C1.1, C1.2, P4.2, P4.3	Inquired of the Program Manager and determined procedures were in place to dispose of confidential information according to the data retention and deletion policies and monitor for resolution of policy violations.	No deviations noted.

bernardoantunes.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
data retention and deletion policy and monitor for resolution of policy violations.		Inspected the organization's internal policies and determined guidelines were established to govern the retention and deletion of user data.	No deviations noted.
		Inspected the deletion monitoring dashboard and configuration for a sample product and determined the monitoring dashboard was used to manage the timeliness of deletion of confidential information as outlined in the data retention and deletion policies and monitor for resolution of policy violations.	No deviations noted.
		Inspected a sample of products and determined an automated deletion mechanism was implemented and confidential information was disposed of as per the data retention and deletion policies.	No deviations noted.
		Inspected a sample product and determined data deletion tools verified that backup data was deleted following the configured retention period, as part of the deletion mechanism process.	No deviations noted.
64. The organization has established policies and guidelines to govern data classification, labeling and security.	CC6.1, C1.1, P4.1	Inquired of the Program Manager and determined the organization has established policies and guidelines to govern data classification, labeling and security.	No deviations noted.
		Inspected relevant documentation and determined the organization established policies and guidelines to govern data classification, labeling and security.	No deviations noted.

bernard@bottomly.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
65. The organization maintains formal user registration and de-registration procedures for granting and revoking access.	CC6.2, CC6.3	Inquired of the Program Manager and determined the organization maintained formal user registration and de-registration procedures for granting and revoking access.	No deviations noted.
		Inspected relevant documentation and determined the organization had formal procedures defining the appropriate use of corporate and production accounts.	No deviations noted.
		Inspected relevant documentation and determined the organization had formal procedures for granting user access to the corporate and production network.	No deviations noted.
		Inspected the relevant guidelines and determined organization maintained formal user de-registration procedures for revoking access for employee's leaving the company.	No deviations noted.
		Observed an attempt to grant user access to a group with the appropriate approval from the group administrator and determined access was granted.	No deviations noted.
		Observed an attempt to grant user access to a group without the appropriate approval from the group administrator and determined access was not granted.	No deviations noted.

bernard@tomorrow.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a terminated user's access to production machines, support tools, network devices and corporate assets and determined access was automatically removed by the automated tool used to revoke access upon submission of a termination request.	No deviations noted.
66. Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	CC6.2, CC6.3	Inquired of the Program Manager and determined that critical access groups were reviewed on a periodic basis by group administrators and inappropriate access was removed.	No deviations noted.
		Inspected relevant documentation and determined that critical access group reviews were done on a periodic basis and scoping was determined accordingly.	No deviations noted.
		Inspected the code configuration and determined that tools used to facilitate the review generated complete and accurate critical access group listings semi-annually and assigned the group administrators.	No deviations noted.
		Inspected a sample of critical access group user membership reviews performed by the appropriate group administrator and determined the review was performed in a timely manner.	Deviations noted. Four (4) of fifty-three (53) critical access groups in the semi-annual review sampled for testing was not performed timely.

bernard@bottaker.net

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Management's Response: Management acknowledges that the periodic access review for 4 selected critical access group was not performed in a timely manner and completed after the defined service level objective (SLO). Management reviewed the memberships to the access groups and determined that there was no inappropriate access identified as result of the delayed review. As per Google's policy, the defined SLO for a review to be completed is 42 days. Reminders are automatically sent to the reviewer at 5, 12, 25, 35, and 41 days. After 25 days, the reviewer's manager is copied on the reminders. If the 42-day SLO has passed, the priority of the review ticket is updated to the highest engineering priority. Management has reiterated the importance of timely completion of the user access reviews to the relevant teams to ensure that reviews are completed within the defined SLO. In addition, the Google security compliance team makes training materials and process documentation readily available to all Google employees.	
		Inspected a sample of users from the review of critical access groups and determined their access was appropriate based on their cost center.	No deviations noted.
		Inspected a sample critical access group user membership review and determined that appropriate action was taken to resolve inappropriate access identified, if applicable.	No deviations noted.

bernard@fatfinke.ie

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample critical access group review and determined they reviewed a complete and accurate listing of critical access groups.	Deviations noted. For twenty-three (23) groups impacting twenty-four (24) products with access to approve or deploy changes to production, were not tagged as critical access groups, hence, were not included in management's review of critical access groups.

bernard@botmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Management's Response: Management reviewed the findings related to the 23 critical access groups for the 24 products that were not included in the periodic access review process, noting the root cause to be an omission resulting from manual error. Management reviewed the memberships to the access groups that were not formally included in the periodic access review process and determined that there was no inappropriate access identified. Further, management has added the 21 of the 23 impacted access groups to the ongoing periodic critical access group review process. For the remaining two (2) impacted groups, key access permissions to edit or write code were removed, hence, would not be tagged as critical access groups. Additionally, Management has assigned compliance specialists to partner with each of the product teams in scope on the design, implementation and testing of security controls. These compliance specialists review the internal control details associated with these products at least annually, with ad hoc reviews as necessary.	
		Inspected a sample critical access group user membership review and determined the review was automatically generated semi-annually.	No deviations noted.
		Inspected a sample critical access group user membership review and determined the review was automatically assigned to a random group owner, the remaining owners are CC'ed and a review link is provided.	No deviations noted.

bernard@[illegible]

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample critical access group user membership review and determined a reminder was automatically generated for an incomplete review.	No deviations noted.
		Inspected a sample critical access group user membership review and determined that when the review is completed within the front-end UI tool provided, the review ticket automatically closed.	No deviations noted.
		Inspected a sample critical access group user membership review and determined the review was automatically assigned to a random Eng Compliance Business Partner if the group owner is unable to be found.	No deviations noted.
67. Where "on demand request" mechanisms are implemented to restrict human access to production resources, access requests are reviewed and approved by a second individual prior to being granted and the event is logged.	CC6.2, CC6.3	Inquired of the Program Manager and determined that "on demand request" mechanisms are implemented to restrict human access to production resources, and "access on demand" requests are reviewed and approved by a second individual prior to being granted and the event is logged.	No deviations noted.
		Inspected relevant documentation and determined that "access on demand" requests are reviewed and approved by an appropriate second individual prior to being granted and that the event is logged.	No deviations noted.

bernardo@atmeet.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the "access on demand" configuration supporting the functionality and determined access requests are configured to restrict human access to production resources via access groups and can only be granted for a limited number of hours.	No deviations noted.
		Observed a user attempt to gain access to an on-demand group and determined access was granted after meeting the predefined conditions (i.e., authorized user request, appropriate approval from a second individual, limited number of hours).	No deviations noted.
		Observed a user attempt to gain access to an on-demand group and determined access was not granted when the predefined conditions (i.e., authorized user request, appropriate approval from a second individual, limited number of hours) were not met.	No deviations noted.
		Inspected a sample of system generated logs and determined that on-demand group transactions were recorded.	No deviations noted.
68. Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).	CC6.2, A1.1, A1.2	Inquired of the Data Center Operations Manager and determined redundant power was utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power sources.	No deviations noted.

bernard@bernsteinr.com

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample of data centers and determined that network rooms were connected to an UPS system and emergency generator power was available for at least 24 hours in the event of a loss of power.	No deviations noted.
		Observed a sample of data centers and determined that data centers were equipped with redundant network connections via different physical connections.	No deviations noted.
		Inspected maintenance records for in-scope data centers and observed that equipment was continuously monitored and periodically tested.	No deviations noted.
69. Visitors to corporate offices must be authenticated upon arrival and remain with an escort for the duration of their visit.	CC6.4	Inquired of the Security Officer and determined that visitors to corporate offices were required to authenticate upon arrival and remain with an escort for the duration of their visit.	No deviations noted.
		Inspected internal documentation and determined the organization maintained policies for visitor access to corporate offices.	No deviations noted.
		Performed inspections for a sample of offices and determined that the reception area was isolated from the office space.	No deviations noted.

bernard@bamoker.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed an on-site sign in of a visitor to Google offices and determined visitors to corporate offices were required to authenticate upon arrival and remain with an escort for the duration of their visit.	Deviation noted. For one (1) of the three (3) offices selected for testing, while there were pre-visit authorization process in place with the Global Security Operations Center (GSOC) team and while the visitor was escorted throughout the visit, there was no authentication process happening upon arrival of the visitor at the office location.

bernard@botmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Management's Response: Management reviewed this finding noting the root cause to be the lack of formal visitor authentication process at the US-POU office. The US-POU is a small office that is currently servicing less than 10 FTEs and has been set up with the expectation that there will only be visitors with a valid business reason. These visitors would be visiting team members, maintenance personnel or external auditors which would be pre-authorized for the visit. Since no other visitors are expected, a formal visitor authentication process was not implemented at this office. Management further reviewed the details of this finding and determined that the extent is limited to the US-POU office. As a result, the residual risk of the visitor impacting the security or reliability of the corporate office is low.	
70. Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	CC6.4	Inquired of the Operations Manager and determined information systems and equipment were safeguarded against unauthorized entry and removal from data centers and data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	No deviations noted.
		Inspected internal documentation and determined that the organization maintains policies and guidelines around the security of storage devices during delivery and movement throughout the data center.	No deviations noted.
		Observed a sample of data centers and determined that Google had safeguards in place to protect information systems and equipment from unauthorized entry and removal from data centers.	No deviations noted.

bernard@pathkey.com

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample of data centers and determined that dedicated receiving and shipping areas were isolated from the main data center floor, network rooms and security systems.	No deviations noted.
		Inspected a sample of tickets created for data center equipment entering and exiting data centers and determined Google authorized, monitored, and controlled the shipments and maintained a record of the items.	No deviations noted.
71. Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.	CC6.4	Inquired of the Data Center Security Manager and determined data center perimeters were defined and secured via physical barriers. Access to sensitive data center zones required approval from authorized personnel and was controlled via badge readers, biometric identification mechanisms, or physical locks.	No deviations noted.
		Observed a sample of data centers and determined that access to sensitive data center facilities required approval from authorized personnel, and required two-factor authentication using badge readers, biometric identification mechanisms or physical locks.	No deviations noted.
		Inspected the Data Center Physical Access Policy and determined access was provisioned on a least-privileged basis and the facilities had segregated security zones.	No deviations noted.

bernardo@bothmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample of data centers and determined that facilities had segregated security zones.	No deviations noted.
		Observed a sample of data centers and determined that data center perimeters were defined and secured via physical barriers.	No deviations noted.
72. Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.	CC6.4	Inquired of the Program Manager and determined user access to high-security areas in data centers was reviewed on a periodic basis and inappropriate access was removed in a timely manner.	No deviations noted.
		Inspected the internal policies and determined user access to high-security areas in data centers was reviewed on a periodic basis.	No deviations noted.
		Inspected a sample of data center access reviews and determined that reviews were performed completely and accurately in a timely manner by appropriate personnel.	No deviations noted.
		Inspected a sample of users marked as appropriate within a data center access review and determined the users were appropriate based on cost center and job title.	No deviations noted.
		Inspected a sample of inappropriate users identified as requiring removal within a data center access review and determined the users were removed in a timely manner.	No deviations noted.

bernard@bmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
73. Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.	CC6.4	Inquired of the Data Center Security Manager and determined visitors were required to gain approval from authorized personnel, have their identity verified and remain with an escort during the duration of their visit.	No deviations noted.
		Inspected the physical security policies and determined the organization required visitors to gain approval from authorized personnel, have their identity verified at the perimeter and remain with an escort during the duration of their visit.	No deviations noted.
		Observed a sample of data centers and determined that individuals on-site had their identities verified before entering the data center floors.	No deviations noted.
		Inspected a sample of access requests to visit data centers and determined approvals were obtained from authorized personnel prior to the visits, and visitors remained with an escort during the duration of their visits.	No deviations noted.
74. Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	CC6.4	Inquired of the Program Manager and determined security measures utilized in data centers were assessed periodically and the results were reviewed by executive management.	No deviations noted.
		Inspected a sample of the reviews performed and determined security measures utilized in all data centers were assessed periodically and the results were reviewed by executive management.	No deviations noted.

bernardabotha@gmail.com

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
75. Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	CC6.4	Inquired of the Data Center Facilities Manager and determined that physical security measures were in place as described and are reviewed through the annual data center security review.	No deviations noted.
		Inspected a sample data center security review performed for the production facilities and determined that management reviewed the physical security measures at the facilities.	No deviations noted.
		Observed a sample of data centers and determined that visitors obtained approvals from authorized personnel prior to their visits, had their identities verified before entering the data center floors, and remained with an escort during the duration of their visits.	No deviations noted.
		Observed a sample of data centers and determined that data centers were continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	No deviations noted.
		Observed a sample of data centers and determined that data centers were secured through the use of badge reader and biometric control systems.	No deviations noted.
		Inspected the badge reader activity logs for a sample of data centers and determined access to Google spaces was logged and monitored.	No deviations noted.

bernard@lothaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the badge reader activity logs for a sample of data centers and determined logs were retained for at least 3 months.	No deviations noted.
76. Data center perimeters are defined and secured via physical barriers.	CC6.4	Inquired of the Data Center Security Manager and determined data center perimeters were defined and secured via physical barriers. Access to sensitive data center zones required approval from authorized personnel and was controlled via badge readers, biometric identification mechanisms, or physical locks.	No deviations noted.
		Observed a sample of data centers and determined that access to sensitive data center facilities required approval from authorized personnel, and required two-factor authentication using badge readers, biometric identification mechanisms or physical locks.	No deviations noted.
		Inspected the Data Center Physical Access Policy and determined access was provisioned on a least-privileged basis and the facilities had segregated security zones.	No deviations noted.
		Observed a sample of data centers and determined that facilities had segregated security zones.	No deviations noted.
		Observed a sample of data centers and determined that data center perimeters were defined and secured via physical barriers.	No deviations noted.

bernardabottah@gmail.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
77. The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.	CC6.4, CC6.7	Inquired of the Data Center Security Manager and determined that the organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.	No deviations noted.
		Inspected the organization's policies and guidelines and determined that physical protection guidelines were specified within each document.	No deviations noted.
78. The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.	CC6.5, P4.3	Inquired of the Operations or Facilities Managers at each site and determined the organization sanitized storage media prior to disposal, release out of organizational control, or release for reuse.	No deviations noted.
		Inspected the data destruction and transportation policies and determined the organization had policies in place regarding the sanitization of storage media prior to disposal, release out of organizational control, or release for reuse.	No deviations noted.
		Inspected the relevant configuration and determined USB ports were disabled at a global level for data centers.	No deviations noted.
		Inspected a sample destroyed equipment leaving the organization's data centers and determined the equipment was subject to the organization's sanitization and destruction process.	No deviations noted.

bernard@stamper.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
79. The organization has implemented perimeter devices to protect the corporate network from external network attacks.	CC6.6	Inquired the Program Manager and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
		Inspected the policies and documents related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
		Inspected the configurations related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
80. Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	CC6.6	Inquired of the Program Manager and determined access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No deviations noted.
		Inspected the configuration and determined access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No deviations noted.
		Inspected a user attempt to access an internal support tool with approved credentials and determined access was granted.	No deviations noted.
		Inspected a user attempt to access an internal support tool without approved credentials and determined access was not granted.	No deviations noted.

bernard@atmen.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
81. Only users with a valid user certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	CC6.6, CC6.7	Inquired of the Program Manager and determined only users with a valid certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	No deviations noted.
		Inspected relevant documentation and determined mechanisms are in place to authenticate users and restrict access to production machines without a valid digital certificate.	No deviations noted.
		Inspected the configuration that enforced the authentication of users prior to granting a private key and determined digital certificates were only generated after a user was authenticated using two-factor authentication.	No deviations noted.
		Inspected a user attempt to access the production machines with an authorized private key by using a valid SSH certificate and determined access was allowed.	No deviations noted.
		Inspected a user attempt to access the production machines without an authorized private key by using an invalid SSH certificate and determined access was denied.	No deviations noted.

bernardo@tinder.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
82. The organization authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items.- -* Deliveries of Assets GPN's IN and Out of DC's	CC6.7	Inquired of the Operations Manager and determined information systems and equipment were safeguarded against unauthorized entry and removal from data centers and data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	No deviations noted.
		Inspected internal documentation and determined that the organization maintains policies and guidelines around the security of storage devices during delivery and movement throughout the data center.	No deviations noted.
		Observed a sample of data centers and determined that that the organization had safeguards in place to protect information systems and equipment from unauthorized entry and removal from data centers.	No deviations noted.
		Observed a sample of data centers and determined that dedicated receiving and shipping areas were isolated from the main data center floor, network rooms and security systems.	No deviations noted.
		Inspected a sample of tickets created for data center equipment entering and exiting data centers and determined the organization authorized, monitored, and controlled the shipments and maintained a record of the items.	No deviations noted.

bernard@bathmake.id

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
83. The organization maintains policies that define the requirements for the use of cryptography.	CC6.7	Inquired of the Program Manager and determined the organization established policies and procedures that govern the internal and external use of cryptographic controls.	No deviations noted.
		Inspected the organization's security policies and procedures and determined they covered governance of the internal and external use of cryptographic controls.	No deviations noted.
		Inspected a Google Cloud Platform relevant documentation and determined they covered governance of the internal and external use of cryptographic controls.	No deviations noted.
84. The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	CC6.7	Inquired of the Program Manager and determined the organization maintained policies for securing mobile devices used to access corporate network and systems.	No deviations noted.
		Inspected relevant policies and documentation and determined the organization maintained policies for securing mobile devices used to access corporate network and systems.	No deviations noted.
85. The organization uses encryption to secure user data in	CC6.7	Inquired of the Program Manager and determined the organization used encryption to secure user data in transit between production facilities.	No deviations noted.

bernard@atmeter.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
transit between the organization's production facilities.		Inspected internal documentation and determined encryption was used to secure user data in transit between the organization's production facilities.	No deviations noted.
		Inspected the encryption configuration and determined encryption was used to secure user data in transit between the organization's production facilities.	No deviations noted.
86. Automated mechanisms are utilized to track inventory of all production machines and inventory of all serialized server components.	CC6.7	Inquired of the Data Center Operations Manager and determined automated mechanisms were utilized to track inventory of production machines.	No deviations noted.
		Inspected the records from the inventory system for a sample of production machines selected during data center inspections and determined the selected machines existed in the inventory system.	No deviations noted.
		Observed a sample of production machines selected from the inventory system prior to the data center inspection and determined that the selected machines existed at the data centers.	No deviations noted.
		Inspected the relevant configuration and determined automated alerts were configured to track inventory of production machines.	No deviations noted.

bernard@bernard.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of alerts generated when thresholds for the organization's inventory tracking processes were exceeded and determined alerts were appropriately generated, responded and resolved in a timely manner.	Deviation noted. For one (1) of twenty-five (25) sampled alert tickets generated to track inventory of production machines, we determined that the ticket was not resolved within the SLO guidelines for the assigned priority and severity.
		Inquired of management and determined if any control deviations were identified during their own internal testing procedures.	Deviation noted. Per review of the first party audit report, for three (3) of twenty-five (25) sampled alert tickets generated to track inventory of production machines, we determined that the ticket was not

bernard@botmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
			resolved within the SLO guidelines for the assigned priority and severity.
		Management's Response: Management acknowledges that four samples, one from EY's testing and three identified by first-party audit, were not resolved within our established internal Service Level Objectives (SLOs). For the sample found from EY's testing, management determined that this deviation was caused due to a delay within a planned dependent project. For three samples from first-party testing, management determined that these deviations were caused by dependent process delays. Throughout their lifecycle, the assets remained secure under multiple layers of physical security with appropriate supervision. These four tickets have since all been fully resolved, and we will continue to review the process of monitoring timely ticket resolution.	
87. Integrity checks are in place at the application level to ensure data integrity.	CC6.7, CC7.1	Inquired of the Program Manager and determined integrity checks were in place via checksum verifications at the application level to help ensure data integrity.	No deviations noted.
		Inspected application level configurations and determined they were configured to use integrity checks via checksum verification.	No deviations noted.

bernard@bottomer.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a user attempt to upload files to a sample application and determined application level integrity checks via checksum verification were in place to help ensure data integrity.	No deviations noted.
88. The organization has established guidelines for governing the installation of software on organization-owned assets.	CC6.7, CC8.1	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
		Inspected the organization's security policies and determined the organization had implemented rules to govern the installation of software by users.	No deviations noted.
		Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
		Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.

bernard@auditboard.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.
		Inquired of the Program Manager and determined that a standard production image was utilized for the installation and maintenance of each production server.	No deviations noted.
		Inspected a sample configuration of the tool the organization uses to monitor the virtual machines and detection of deviations for the virtual machine.	No deviations noted.

bernard@bethmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of tickets and determined that deviations identified in virtual machines are detected and corrected.	No deviations noted.
89. The organization prohibits the use of removable media for the storage of PII and SPII unless the data has been encrypted.	CC6.7, P4.3	Inquired of the Program Manager and determined PII and SPII on removable media leaving the organization's facilities was approved and encrypted.	No deviations noted.
		Inspected relevant policies and determined the organization outlined and communicated the process for the secure handling and transportation of customer data.	No deviations noted.
		Inspected the ticketing tool and determined requests to use removable media were approved under the condition that the removable media was encrypted.	No deviations noted.
90. The organization has implemented mechanisms to protect its information assets against malicious activity (e.g. malware, spam, phishing).	CC6.8	Inquired of the Program Manager and determined the organization has implemented mechanisms to protect its information assets against malicious activity.	No deviations noted.
		Inspected Google's internal guidelines and determined the organization has implemented mechanisms to protect its information assets against malicious activity.	No deviations noted.
		Inspected the antivirus and antimalware mechanisms and determined that the tools were in place to protect the organization's information assets.	No deviations noted.

bernard@bernard.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected internal documentation and determined antivirus software in place was configured to have a function to roll-back to a previous state in case of malfunction of an anti-virus system update.	No deviations noted.
91. Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.	CC6.8	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
		Inspected Google's security policies and determined Google had implemented rules to govern the installation of software by users.	No deviations noted.
		Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
		Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.

bernardo@google.com

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.
		Inquired of the Program Manager and determined that a standard production image was utilized for the installation and maintenance of each production server.	No deviations noted.
		Inspected a sample configuration of the tool Google uses to monitor the virtual machines and detection of deviations for the virtual machine.	No deviations noted.

bernard@bernaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of tickets and determined that deviations identified in virtual machines are detected and corrected.	No deviations noted.
92. The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	CC6.8, CC7.1, CC7.3, A1.1	Inquired of the program manager and determined the organization provided monitoring tools to facilitate the detection and reporting of operational issues and the monitoring tools sent automated alerts to operational personnel based on predetermined criteria and are escalated per policy.	No deviations noted.
		Inspected relevant documentation and determined there were tools in place to detect and report operational issues to operational personnel.	No deviations noted.
		Inspected a sample of alerts and determined monitoring tools were in place to detect, report, escalate and resolve operational issues.	No deviations noted.
		Inspected evidence of escalated sample security incident and determined appropriate action was taken to identify, record, track and resolve the incident in a timely manner.	No deviations noted.
93. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	CC6.8, CC7.2, CC7.3, CC7.4,	Inquired of the program manager and determined the organization provided monitoring tools to facilitate the detection and reporting of operational issues and the monitoring tools sent automated alerts to operational personnel based on predetermined criteria and are escalated per policy.	No deviations noted.

bernardo@bottomline.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
	CC7.5, CC8.1, A1.1	Inspected relevant documentation and determined there were tools in place to detect and report operational issues to operational personnel.	No deviations noted.
		Inspected a sample of alerts and determined monitoring tools were in place to detect, report, escalate and resolve operational issues.	No deviations noted.
		Inspected evidence of escalated sample security incident and determined appropriate action was taken to identify, record, track and resolve the incident in a timely manner.	No deviations noted.
94. The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	CC7.1	Inquired of the Program Manager and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	No deviations noted.
		Inspected the internal documentation and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the network	No deviations noted.
95. Integrity checks are in place at the file system level to ensure data integrity.	CC7.1	Inquired of the Program Manager and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.
		Inspected the organization's security policies and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.

bernard@ethaler.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations to ensure data integrity at the file system level.	No deviations noted.
		Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration to ensure data integrity at the file system level.	No deviations noted.
		Observed a Software Engineer insert a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
		Observed a Software Engineer modify a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
		Observed a Software Engineer delete a sample file in the directory of a haphazardly selected production machine and determined the tool detected the deleted sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.

bernard@hotmail.com

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
96. Logical access to network devices is restricted to authorized personnel and is periodically reviewed.	CC7.1	Inquired of the Program Manager and determined that access to network devices was restricted to authorized personnel and periodically reviewed.	No deviations noted.
		Inspected the network device access management policy and determined access to network devices was restricted to authorized personnel and periodically reviewed.	No deviations noted.
		Inspected a sample user provisioned and deprovisioned access and determined that logical access was restricted to authorized personnel.	No deviations noted.
		Inspected source code and determined logical access to network devices is restricted to authorized personnel via access rules.	No deviations noted.
		Inspected a sample of semi-annual user access reviews performed for network devices and determined the reviews were performed timely and by appropriate personnel and any changes needed were made.	No deviations noted.
97. The organization makes procedures related to the management of information processing resources available. Procedures include guidance on requesting, monitoring and	CC7.1, CC7.2, CC7.3, CC7.4, CC7.5	Inquired of the Program Manager and determined the organization made available, procedures related to the management of information processing resources. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	No deviations noted.

bernard@mantmark.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
maintaining resources, and guidance around evaluating capacity demand.		Inspected the organization's resource management documentation and determined an overview to monitor, maintain and evaluate storage and processing capacity demand had been provided.	No deviations noted.
		Inspected a sample monitoring dashboard and determined they are used to monitor and manage capacity of its information processing resources. Inspected a sample of automated notifications related to critical resource capacity utilization and determined alerts were appropriately set.	No deviations noted.
98. The organization has implemented mechanisms to protect the production environment from denial of service attacks.	CC7.2	Inquired of the Program Manager and the Security Reliability Engineer and determined there were mechanisms in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
		Inspected the documentation for mechanisms that are used to protect against denial of service attacks and determined they were in place to protect the production environment.	No deviations noted.
		Inspected playbooks used by the incident management teams and determined mechanisms were in place to classify, escalate and triage denial of service attacks.	No deviations noted.

bernard@bernard.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the DOS server configuration and determined configurations were in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
		Inspected a sample of denial of service attacks and determined mechanisms were in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
		Inspected the dashboards for a sample of in-scope applications and determined monitoring mechanisms were in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
99. The organization has a dedicated team responsible for managing security and privacy incidents.	CC7.2, CC7.3, CC7.4, CC7.5, A1.3, P6.3	Inquired of the Program Manager and determined the organization had a dedicated team responsible for managing security and privacy incidents, and provides internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.
		Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.

kmarchantmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected relevant documentation and determined the organization provided internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.
		Observed the organization's incident management ticketing system and determined that mechanisms were in place to track internal and external reported security and privacy incidents through investigation and resolution.	No deviations noted.
100. Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	CC7.2, CC7.3, CC7.4, C1.1	Inquired of the Security Engineering Manager and determined audit logs were continuously monitored for events related to security, availability, processing integrity and confidentiality threats and alerts are generated for further investigation.	No deviations noted.
		Inspected internal documentation and determined there are guidelines used by the Security Surveillance Team to classify, prioritize, perform cause analysis, and triage the security incidents.	No deviations noted.
		Inspected internal documentation and determined the organization provides logging capabilities to its customers and customers can only access records related to their own activities.	No deviations noted.

bernard@bottomer.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample log configuration and determined log sources were monitored and maintained to continuously detect malicious or unusual insider activity.	No deviations noted.
		Observed a sample of alerts for events related to security, availability, processing integrity and confidentiality and determined alerts were generated when the pre-defined criteria was met.	No deviations noted.
		Observed the dashboard of monitoring tools and determined that alerts related to security, availability, processing integrity and confidentiality were monitored.	No deviations noted.
		Inspected that emergency changes are logged and subject to automated checks.	No deviations noted.
		Inspected a sample of emergency changes that required manual investigation and determined whether they were appropriately resolved.	No deviations noted.
101. The organization maintains a framework that defines how to organize a response to security and privacy incidents.	CC7.3, CC7.4, P6.3	Inquired of the Program Manager and determined the organization maintained a framework that defined how to organize a response to security and privacy incidents.	No deviations noted.
		Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.

bernard@anthropic.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected relevant documentation and determined a process was in place for incident response teams to quantify, manage and monitor incidents.	No deviations noted.
102. The organization provides internal personnel (employees and extended workforce) with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	CC7.3, CC7.4, P6.3	Inquired of the Program Manager and determined the organization had a dedicated team responsible for managing security and privacy incidents, and provides internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.
		Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.
		Inspected relevant documentation and determined the organization provided internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.
		Observed the organization's incident management ticketing system and determined that mechanisms were in place to track internal and external reported security and privacy incidents through investigation and resolution.	No deviations noted.

bernardobourrat.vio

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
103. The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	CC7.3, CC7.4, P6.3, P6.6	Inquired of the Program Manager and determined the organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	No deviations noted.
		Inspected relevant documentation and determined procedures existed for users to prepare, report and investigate security and privacy incidents.	No deviations noted.
		Inspected the Cloud Data Processing Amendment and determined policies and procedures existed to notify customers of an incident in a timely manner and in accordance with applicable laws.	No deviations noted.
		Inspected a sample of data incidents and determined customers were notified of data incidents in a timely manner when required by applicable laws or contractual agreements.	No deviations noted.
		Inspected the public dashboards and tools available to customers and determined customers were notified of outages and incidents that impact relevant services.	No deviations noted.
104. The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support	CC7.4, A1.1, A1.2, A1.3	Inquired of the Program Manager and determined the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	No deviations noted.

bernard@trainer.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
service redundancy, and availability.		Inspected a sample datastore configuration for a Google Cloud Platform product and determined the product was configured to replicate to support service redundancy, and availability.	No deviations noted.
		Inspected the Google Cloud Platform product's monitoring dashboard and determined resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy.	No deviations noted.
		Inspected the Google Cloud Platform product's monitoring dashboard and determined resources were distributed across distinct, geographically dispersed processing facilities to support service availability.	No deviations noted.
105. Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	CC7.5	Inquired of the Program Manager and determined information security incidents were documented per the organization's Incident Response Policy. Information from these events could be used to prevent future incidents and as examples for information security training.	No deviations noted.
		Inspected the organization's incident response policies and determined it documented the process for reporting, responding to, and monitoring information security incidents.	No deviations noted.

bernardo@ernst.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected relevant internal documentation and determined information security trainings were implemented and that incidents were analyzed to prevent future incidents.	No deviations noted.
106. Development, testing and build environments are separated from the production environment through the use of logical security controls.	CC8.1	Inquired of the Program Manager and determined the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
		Inspected internal documentation and determined the organization maintained separate development, testing, and production environments.	No deviations noted.
		Inspected the relevant code and determined that builds deployed into production are systematically verified prior to deployment or have a valid exception.	No deviations noted.
		Observed that manual builds must still be submitted, reviewed and systematically verified prior to deployment to production.	No deviations noted.
		Inspected security and access restriction settings for a sample of products related to the change pipeline for services running in the organization's production environment, and determined that the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.

bernard@anthropic.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected security and access restriction settings for a sample of products related to the change pipeline for open source code packages maintained in a public source code repository, and determined that the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
		Inspected security and access restriction settings for a sample of products related to the change pipeline for images, downloads, or software updates made available to customers, and determined that the organization separated development, testing, and build environments from production through the use of logical security controls.	Deviations noted. For three (3) of fifty-eight (58) products sampled for testing, sixteen (16) users with admin/write access within development, testing, and build registries prior to deployment were not added to either critical access groups (CAGs) or on-demand groups. As such, users were not controlled through the use of logical security controls governing

bernard@ntpaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
			CAGs and on-demand groups.
		Management's Response: Management acknowledges that for 3 identified products, 16 users had direct access to resources within the software deployment process, such as build repositories. Although the control process over separation of development, testing, and build environments from production through the use of logical security controls is common across different Google products, management identified that the two (2) of the three (3) impacted sample products changes were related to Apigee and Data products. The remaining one (1) product is not related to Google Cloud Platform. Management determined that access to these resources is expected to be provided through critical access groups (CAGs) or on-demand groups. This deviation occurred as a result of teams incorrectly provisioning access at the user level rather than the group level and was an oversight. Further, management conducted a comprehensive review of users with access to these resources and direct user access has been revoked. The direct user access had not resulted in unauthorized changes to production and there was no impact to production resources. Access has been appropriately restricted to designated groups which are managed as a part of Google's established access control procedures. Additionally, management noted that Control 15 of the report related the enforcement of multi-party approval for code changes would further mitigate the risk associated with this finding.	

bernard@attmail.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample Google Cloud Platform change and determined the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
107. The organization has policies and guidelines governing the secure development lifecycle.	CC8.1	Inquired of the Program Manager and determined the organization had policies and procedures which govern the secure development lifecycle.	No deviations noted.
		Inspected internal documentation and determined the organization had policies and procedures which govern the secure development lifecycle.	No deviations noted.
108. Changes to the organization's systems are tested before being deployed.	CC8.1	Inquired of the Program Manager and determined that application and configuration changes are tested, validated, and documented prior to deployment to production.	No deviations noted.
		Inspected the associated ticket details for a sample of product application and configuration changes related to services running in the organization’s production environment, and determined that the changes were tested, validated, and documented prior to implementation to production.	No deviations noted.

bernard@[illegible]

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the associated ticket details for a sample of product application and configuration changes related to open source code packages maintained in a public source code repository, and determined that the changes were tested, validated, and documented prior to implementation to production.	Deviations noted. For four (4) samples of the twenty-five (25) sampled changes selected for testing, documentation was not retained to evidence the testing performed in the staging environment prior to deployment to production.
		Management's Response: Management acknowledges that four (4) selected sample changes lacked evidence of testing conducted in the staging environment prior to production deployment. Although the control process over testing of changes prior to deployment is common across different Google products, management identified that the 4 impacted sample changes were not related to Google Cloud products. Management also determined that these changes were tested in the staging environment, but evidence of this testing was not subsequently recorded in the test log. Further, management performed a comprehensive review of the 4 changes and determined that the changes were valid, with no impact on production resources. Two (2) of the changes involved parameter adjustments to open-source code, and the remaining two (2) were minor database configuration	

bernard@botmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		updates. Management reiterated the importance of following change management policies to ensure that changes are tested and documented prior to production deployment. Additionally, management identified the four changes were validated and approved by a second engineer prior to production deployment as tested in Control 15 in the report.	
		Inspected the associated ticket details for a sample of product application and configuration changes related to images, downloads, or software updates made available to customers, and determined that the changes were tested, validated, and documented prior to implementation to production.	No deviations noted.
109. Changes to network configurations are reviewed and approved prior to deployment.	CC8.1	Inquired of the Program Manager and determined changes to network configurations were reviewed, approved, and tested prior to deployment.	No deviations noted.
		Inspected a sample of manual network configuration changes and determined they were reviewed by a separate technical resource to validate quality and accuracy.	No deviations noted.
		Inspected a sample of manual network configuration changes and determined they were tested prior to deployment.	No deviations noted.

bernardoimarket.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample automated change and determined it was made by an automated tool based on the pre-configured ruleset.	No deviations noted.
		Inspected a sample of changes made to the automated tool and determined it was reviewed by a separate technical resource to validate quality and accuracy and tested prior to deployment.	No deviations noted.
110. A standard image is utilized for the installation and maintenance of each production server.	CC8.1	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
		Inspected Google's security policies and determined Google had implemented rules to govern the installation of software by users.	No deviations noted.
		Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.

bernardo@tomelo.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
		Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.

bernardabbottnv@gmail.com

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inquired of the Program Manager and determined that a standard production image was utilized for the installation and maintenance of each production server.	No deviations noted.
		Inspected a sample configuration of the tool Google uses to monitor the virtual machines and detection of deviations for the virtual machine.	No deviations noted.
		Inspected a sample of tickets and determined that deviations identified in virtual machines are detected and corrected.	No deviations noted.
111. The organization requires external parties (Service Providers) to meet security and privacy requirements for safeguarding user data. Requirements are enforced via the “Information Protection Addendum (IPA)” or “Partner Information Protection Addendum (PIPA)” for vendors/service providers and partners, respectively.	CC9.1	Inquired of the Program Manager and determined the organization required external parties (Service Providers) to meet security and privacy requirements for safeguarding user data and the requirements were enforced via the “Information Protection Addendum (IPA)” or “Partner Information Protection Addendum (PIPA)” for providers and partners, respectively.	No deviations noted.
		Inspected relevant documentation and determined the organization had a formal due diligence process in place for engaging with third parties.	No deviations noted.
		Inspected the Information Protection Addendum (IPA) template and determined appropriate information security and data protection terms were documented within the IPA.	No deviations noted.

bernard@bernard.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the Partner Information Protection Addendum (PIPA) template and determined appropriate information security and data protection terms were documented within the PIPA.	No deviations noted.
		Inspected a sample Vendor that processes Google customer data and determined that they had signed an Information Protection Addendum (IPA) or Partner Information Protection Addendum (PIPA).	No deviations noted.
112. The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	CC9.1, A1.2, A1.3	Inquired of the Program Manager and determined that the organization conducted disaster resiliency testing (DiRT) which covered reliability, survivability, and recovery on an ongoing basis (and at least annually).	No deviations noted.
		Inspected a sample of the functional disaster resiliency testing documentation and determined that it was conducted on a periodic basis and testing was conducted to ensure continuous and automated disaster readiness, response, and recovery of business, systems and data.	No deviations noted.
		Inspected testing documentation and determined that product teams developed testing plans and postmortems which documented the results and lessons learned from disaster resiliency testing.	No deviations noted.

bernardapathfinder.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
113. The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	CC9.1, A1.2, A1.3	Inquired of the Program Manager and determined that the organization had implemented business continuity measures to maintain the availability of the organization's production infrastructure and services.	No deviations noted.
		Inspected internal documentation and determined that the organization defined the risks and recovery objectives to establish measures that maintain the availability of its production infrastructure and services.	No deviations noted.
		Inspected the documentation that establishes measures to maintain the availability of the organization's production infrastructure and services.	No deviations noted.
		Inspected the documentation that establishes measures to maintain the availability of the organization's production infrastructure and services and determined the documentation was tested on an interval basis or upon significant organizational or environmental changes.	No deviations noted.
		Inspected a sample of team or product area guidelines available and determined it included the procedures which need to be followed in an emergency or incident.	No deviations noted.
		Inspected a sample of tickets and determined recovery activities were outlined.	No deviations noted.

bernard@[illegible]

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
114. The organization maintains business continuity plans to define how personnel should respond to disruptions.	CC9.1, A1.2, A1.3	Inquired of the Program Manager and determined the organization maintains business continuity plans to define how personnel should respond to disruptions.	No deviations noted.
		Inspected internal websites and determined that business continuity plans were maintained and made available to corresponding data center teams for organization-owned and third-party data centers.	No deviations noted.
		Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample of the Organization-owned data centers and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.
		Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample third-party data center and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.
115. The organization has policies and guidelines that govern third-party relationships.	CC9.2	Inquired of the Program Manager and determined the organization developed policies and guidelines that govern third party relationships.	No deviations noted.
		Inspected internal documentation and determined policies and guidelines were in place to govern third party relationships.	No deviations noted.

bernard@atmore.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
116. Subprocessor performance is regularly assessed and monitored via periodic business reviews	CC9.2	Inquired of the Program Manager and determined subprocessor performance was regularly assessed and monitored via periodic business reviews.	No deviations noted.
		Inspected documentation for a sample of subprocessors and determined that subprocessor performance was regularly assessed and monitored via periodic business reviews.	No deviations noted.
117. The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	CC9.2, C1.1	Inquired of the Program Manager and determined the organization had established agreements, including non-disclosure agreements, for preserving confidentiality of information and software exchanges with external parties, such as third-party vendors.	No deviations noted.
		Inspected relevant documentation and determined the organization had established agreements in place, including non-disclosure agreements, for preserving confidentiality of information and software exchanges with external parties, such as third-party vendors.	No deviations noted.
		Inspected the latest non-disclosure agreement template and determined the organization had established agreements with external parties for preserving confidentiality of information and software exchanges.	No deviations noted.

bernard@tomoki.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected agreements for a sample of external parties and determined the organization had signed non-disclosure agreements for preserving confidentiality of information and software exchanges with external parties.	No deviations noted.
118. The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	CC9.2, C1.1	Inquired of the Program Manager and determined the organization required its extended workforce personnel to sign confidentiality agreements that defined responsibilities and expected behavior for the protection of information.	No deviations noted.
		Inspected the organization's confidentiality agreements and determined they defined extended workforce personnel responsibilities and expected behavior for the protection of information.	No deviations noted.
		Inspected a sample extended workforce personnel and determined they signed the confidentiality agreements, indicating their acceptance of the responsibilities and expected behavior in regards to protection of information.	No deviations noted.
119. The Privacy, Safety Security Org (PSS) takes a risk based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual	CC9.2, C1.1	Inquired of the Program Manager and determined that the Privacy, Safety Security Org (PSS) takes a risk based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	No deviations noted.

bernard@banker.ie

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
assessment as determined by the sensitivity of data being processed or access being granted.		Inspected the relevant documentation and determined the Privacy, Safety Security Org (PSS) took a risk based approach to reviewing the security practices of vendors and the security posture of vendor products, including automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	No deviations noted.
		Inspected a sample of vendors and determined the security practices of vendor and the security posture of vendor products were reviewed.	No deviations noted.
120. The organization has established confidentiality agreements that are reviewed (by regional Employment Legal teams) and updated (by Google's regional Offer Letter teams), as needed.	CC9.2, C1.1	Inquired of the Program Manager and determined confidentiality agreements for employees and third parties are reviewed and updated as needed.	No deviations noted.
		Inspected the confidentiality agreements and determined they were reviewed and updated by the organization as needed.	No deviations noted.
121. The organization requires subprocessors to meet security and privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are	CC9.2, C1.1, P6.1, P6.4, P6.5, P6.6	Inquired of the Program Manager and determined the organization required subprocessors to meet security and privacy requirements for safeguarding user data and the requirements were enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements.	No deviations noted.

bernard@bellmarket.ie

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
enforced via the “Subprocessor Data Protection Agreement (SDPA)” addendum to contractual agreements or other data processing terms.		Inspected the addendum template and determined it defined the security and privacy obligations that subprocessors must meet to satisfy the organization's obligation regarding customer data.	No deviations noted.
		Inspected the addendum template and determined that appropriate exception handling procedures for service or product issues related to vendors were in place.	No deviations noted.
		Inspected a sample of subprocessors and determined that the subprocessors had a signed SDPA in place in addition to their contractual agreements to enforce security and privacy requirements.	No deviations noted.
122. Cloud Subprocessor security and privacy risk is assessed via periodic assessment of sub-processor control environment.	CC9.2, P6.1, P6.4	Inquired of the Program Manager and determined Cloud subprocessor security and privacy risk was assessed via periodic assessment of subprocessor control environment.	No deviations noted.
		Inspected documentation of a review for a sample of subprocessors and determined that assessments of their security and privacy controls were performed on a periodic basis	No deviations noted.
123. Critical power and telecommunications equipment in data centers is physically	A1.2	Inquired of the Operations Manager and determined critical power and telecommunications equipment in data centers were physically protected from disruption and damage.	No deviations noted.

bernard@katmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
protected from disruption and damage.		Observed a sample of data centers and determined that power and telecommunications equipment in data centers were physically protected from disruption and damage.	No deviations noted.
		Observed a sample of data centers and determined that temperature and humidity of data halls were within the configured thresholds.	No deviations noted.
124. Data centers are equipped with fire detection alarms and protection equipment.	A1.2	Inquired of the Data Center Operations Facilities Manager and determined data centers were equipped with fire detection alarms and protection equipment.	No deviations noted.
		Observed a sample of data centers and determined that they were equipped with fire detection alarms and protection equipment.	No deviations noted.
		Observed a sample of data centers and determined that potential environmental threats to the data centers were anticipated and countermeasures were established based on the nature and geographical location of the data centers.	No deviations noted.
125. Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	C1.1	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.

bernard@datamaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
		Inspected a sample product launch and determined a design document and privacy review were completed prior to the launch.	No deviations noted.
		Inspected a sample of official product blogs for product and feature releases and determined relevant personnel and impacted customers were notified.	No deviations noted.
126. The organization performs privacy reviews prior to product launch.	C1.1, P3.1	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.
		Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
		Inspected a sample product launch and determined a design document and privacy review were completed prior to the launch.	No deviations noted.
		Inspected a sample of official product blogs for product and feature releases and determined relevant personnel and impacted customers were notified.	No deviations noted.

bernard@bobmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
127. The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	C1.2, P1.1, P2.1, P4.2, P4.3	Inquired of the Program Manager and determined the organization maintained policies regarding the return, transfer, and disposal of user data and made these policies available to customers.	No deviations noted.
		Inspected publicly available documentation for Cloud and determined the organization had policies regarding the return, transfer, and disposal of user data and made these policies available to customers.	No deviations noted.
		Inspected the organization's internal policies and determined guidelines were established to govern the retention and deletion of user data.	No deviations noted.
		Inspected a sample deleted file and determined an automated deletion mechanism was implemented and confidential information was disposed of as per the guidelines.	No deviations noted.
128. Where the organization is a data processor, the organization limits scope of processing to what is specified in contracts with the controller.	P1.1, P2.1, P3.1, P3.2, P4.1, P4.2, P7.1	Inquired of the Program Manager and determined the organization limited the scope of processing to what was specified in contracts with the controller.	No deviations noted.
		Inspected externally published documentation and determined the organization provided notice to data subjects about its privacy practices with consent obtained for the use of personal information and the organization limited the scope of processing to what was specified in contracts with controller.	No deviations noted.

bernard@anthem.ai

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected internal documentation and determined the organization limited the scope of processing to what was specified in contracts with the controller.	No deviations noted.
		Observed a user upload data to Google Cloud Platform Services and determined that Google did not use the customer provided content for purposes not specified in the data processing addendum (e.g., advertising).	No deviations noted.
129. The organization only processes user data in accordance with the applicable data processing terms and does not process user data for any other purpose.	P1.1, P3.1, P4.1	Inquired of the Program Manager and determined that customer data was only processed in accordance with the data processing terms and not for any other purpose.	No deviations noted.
		Inquired of Product Counsel Program Manager and determined the new products and features were reviewed prior to launch to confirm products and services were designed to only process customer data in accordance with the data processing addendum and not for any other purpose.	No deviations noted.
		Inspected the Cloud Data Processing and Security Terms and determined that the organization only processed customer data in accordance with the applicable data processing terms and not for any other purpose.	No deviations noted.

bernard@tradmerit.io

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a user upload data to Google Cloud Platform Services and determined that the organization did not use the customer provided content for purposes not specified in the data processing addendum (e.g., advertising).	No deviations noted.
130. Customers of the organization's services are provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.	P5.1, P5.2	Inquired of the Program Manager and determined that Customers of the organization's services were provided a mechanism to access, correct, and erase PII created by their accounts.	No deviations noted.
		Inspected the Google Cloud Data Processing Terms and relevant technical guides and determined that Customers of the organization's services were provided a mechanism to access, correct, and erase PII created by their accounts.	No deviations noted.
		Observed the Google Cloud Platform Console and determined users have the ability to access, correct, and erase PII created by their account.	No deviations noted.
131. A service administrator is provided a mechanism to facilitate a service user's right to access, correct, and erase Customer Data pertaining to the user, consistent with the functionality of the services.	P5.1, P5.2	Inquired of the Program Manager and determined a Google service administrator was provided a mechanism to facilitate a Google service user's right to access, correct, and erase PII pertaining to the user.	No deviations noted.
		Inspected the Data Processing Terms and Terms of Service and determined that Google provides the mechanism to facilitate customer's ability to access, correct and erase PII pertaining to the user.	No deviations noted.

bernardoboatmaker.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample GCP product and determined service administrators had a mechanism to facilitate a user's ability to access, correct, and erase PII pertaining to the user.	No deviations noted.
132. Where the organization is a data processor, the organization has policies regarding its obligations to customers' ability to access, correct and/or erase their user data.	P5.1, P5.2, P6.7, P7.1	Inquired of the Program Manager and determined the organization had policies regarding its obligations to customers' ability to access, correct, and/or erase their user data.	No deviations noted.
		Inspected relevant documentation and determined the organization had policies regarding its obligations to customers' ability to access, correct, and/or erase their user data.	No deviations noted.
133. Where the organization is a data processor, the organization maintains and makes available a list of subprocessors and updates that list, as contractually required.	P6.1, P6.4	Inquired of the Program Manager and determined that where the organization is a data processor, the organization maintained and made available a list of subprocessors and updated that list, as contractually required.	No deviations noted.
		Inspected the organization's public-facing website and determined an updated list of all subprocessors was publicly available, as contractually required.	No deviations noted.
		Inspected a sample email notification and determined notice of subprocessor changes were sent to customers.	No deviations noted.

bernard@gmail.com

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample notification to customers from Professional Services Organizations (PSOs) and determined customers were made aware of the subprocessors used for their project.	No deviations noted.
134. The organization reviews government agency requests for user data to determine if disclosure is required; subsequent disclosure is then limited only to that which is necessary to fulfill the request.	P6.1, P6.4	Inquired of the Program Manager and determined the organization reviewed government agency requests for customer data to determine if disclosure is required; subsequent disclosure was then limited only to that which was necessary to fulfill the request. The organization recorded and tracked transfers and disclosures of user data to third parties.	No deviations noted.
		Inspected the Google Cloud Platform Terms of Service and determined the organization was required to review government agency requests for customer data to determine if disclosure was required; subsequent disclosure was then limited only to that which was necessary to fulfill the request.	No deviations noted.
		Inspected a sample of disclosure requests in the legal request management tool and determined the organization recorded and tracked transfers and disclosure of data to third parties, and the disclosures were limited to only that which was necessary to fulfill the request.	No deviations noted.

bernard@bernard.ie

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
135. Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon in the contract, unless such notification is otherwise prohibited.	P6.1, P6.7	Inquired the Program Manager and determined that customers were notified of data requests from government agencies in accordance with the procedure and time period agreed upon in the contract, unless such notification was otherwise prohibited.	No deviations noted.
		Inspected the Google Cloud Platform Terms of Service and other publicly available documentation and determined they outlined the procedures the company follows to notify customers when disclosure of customer data was legally required.	No deviations noted.
		Inspected the organization's internal website and determined the organization had established mechanisms to ensure customers were notified in accordance with the terms of service when a disclosure of customer data was legally required.	No deviations noted.
		Inspected the configuration supporting the automatic creation of data requests within the organizations internal tools to validate that data requests from government agencies are tracked and managed.	No deviations noted.
		Inspected a sample of disclosure requests and determined notification was sent to the customers in accordance with contractual requirements.	No deviations noted.

bernard@bernard.net

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
136. The organization records requests to disclose user data. The organization's records of requests for user data include information regarding when the request was submitted, the identity of the requester, user data that was requested, any data that had been disclosed, and when disclosure had occurred.	P6.2	Inquired of the Program Manager and determined the organization reviewed government agency requests for customer data to determine if disclosure is required; subsequent disclosure was then limited only to that which was necessary to fulfill the request. The organization recorded and tracked transfers and disclosures of user data to third parties.	No deviations noted.
		Inspected the Google Cloud Platform Terms of Service and determined the organization was required to review government agency requests for customer data to determine if disclosure was required; subsequent disclosure was then limited only to that which was necessary to fulfill the request.	No deviations noted.
		Inspected a sample of disclosure requests in the legal request management tool and determined the organization recorded and tracked transfers and disclosure of data to third parties, and the disclosures were limited to only that which was necessary to fulfill the request.	No deviations noted.
137. The organization has an incident response program for responding to privacy incidents. Privacy incidents are monitored	P6.3, P6.5	Inquired of the Program Manager and determined the organization had an incident response program in place for responding to privacy incidents. Privacy incidents were monitored and tracked in accordance with internal policy.	No deviations noted.

bernardo@stepaside.net

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
and tracked in accordance with internal policy.		Inspected internal documentation and determined the organization had an incident response program in place for responding to privacy incidents.	No deviations noted.
		Inspected a sample incident and determined that the organization had tools and dashboards available and used them to monitor and track incidents in accordance with internal policy.	No deviations noted.
138. Where the organization is a data processor, the organization maintains the necessary records of processing in accordance with contractual obligations to controllers.	P6.7	Inquired of the Program Manager and determined where the organization was a data processor, the organization maintained the necessary records of processing in accordance with the contractual obligations to controllers.	No deviations noted.
		Inspected the Cloud Data Processing Addendum and other internal documentation and determined where the organization was a data processor, the organization maintained the necessary records of processing in accordance with the contractual obligations to controllers.	No deviations noted.
		Inspected a sample processor record of processing for Google Workspace and Google Cloud Platform and determined the organization maintained the necessary records of processing in accordance with the contractual obligations to controllers.	No deviations noted.

bernardo@trail.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
139. Action items identified from the results of internal audit control testing are assigned an owner and tracked to ensure remediation.	P8.1	Inquired of the Program Manager and determined action items identified from the results of internal audit control testing were assigned an owner and tracked to ensure remediation.	No deviations noted.
		Inspected the internal audit report and determined action items identified from the results of internal audit control testing were assigned an owner and tracked to ensure remediation.	No deviations noted.
		Inspected action items from prior period internal audit testing and determined they were tracked to ensure remediation.	No deviations noted.
140. The organization's privacy program is periodically reviewed for appropriateness.	P8.1	Inquired of the Program Manager and determined the organization's privacy program was periodically reviewed for appropriateness.	No deviations noted.
		Inspected internal documentation and determined the organization's privacy program was periodically reviewed for appropriateness.	No deviations noted.
		Inspected the Internal Audit report and determined the organization's privacy program was periodically reviewed by Internal Audit for effectiveness.	No deviations noted.
141. The organization has established feedback processes that give external users the ability	P8.1	Inquired of the Program Manager and determined Google has an established feedback processes that gives external users the ability to voice privacy concerns, which are monitored.	No deviations noted.

bernard@anthropic.io

Google Confidental Information

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
to voice privacy concerns, which are monitored.		Inspected Google's publicly available Help and Support page and determined external users have the option to voice privacy concerns to Google.	No deviations noted.
		Inspected Google's internal website and determined Google has established guidelines that customer support employees used to provide feedback to external users.	No deviations noted.
		Inspected a sample of inquiries, complaints, and disputes, and determined the cases were addressed and resolutions were monitored through to resolution.	No deviations noted.
142. Internal Audit performs a periodic assessment of privacy controls. Results are shared as necessary and are considered for ongoing improvement of the privacy program.	P8.1	Inquired of the Program Manager and determined Internal Audit performed a periodic assessment of privacy controls. Results were shared as necessary and were considered for ongoing improvement of the privacy program.	No deviations noted.
		Inspected internal documentation and determined Internal Audit was responsible for performing a periodic assessment of Google's privacy controls.	No deviations noted.
		Inspected the Internal Audit report and determined Internal Audit performed a periodic assessment of privacy controls. Results were shared as necessary and were considered for ongoing improvement of the privacy program.	No deviations noted.

bernard@lotmark.io

Google Confidental Information

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC1.1 - COSO Principle 1		
CC1.1	1, 2, 3, 4, 5	The entity demonstrates a commitment to integrity and ethical values.
CC1.2 - COSO Principle 2		
CC1.2	6	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3 - COSO Principle 3		
CC1.3	7, 8, 9	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4 - COSO Principle 4		
CC1.4	2, 3, 7, 8	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5 - COSO Principle 5		
CC1.5	4, 6, 9, 10, 11	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.1 - COSO Principle 13		
CC2.1	12, 13, 14, 15	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2 - COSO Principle 14		
CC2.2	3, 9, 13, 14, 16, 17, 18, 19, 20	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3 - COSO Principle 15		
CC2.3	17, 18, 21, 22, 23, 24	The entity communicates with external parties regarding matters affecting the functioning of internal control.

bernard@tetmaster.io

Google Confidental Information

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC3.1 - COSO Principle 6		
CC3.1	9, 25, 26, 27, 28	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2 - COSO Principle 7		
CC3.2	25, 26, 27, 28, 29, 30, 31	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3 - COSO Principle 8		
CC3.3	25, 26, 27, 28, 30	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4 - COSO Principle 9		
CC3.4	25, 26, 27, 28	The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.1 - COSO Principle 16		
CC4.1	11, 32, 33, 34	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2 - COSO Principle 17		
CC4.2	11, 33	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
CC5.1 - COSO Principle 10		
CC5.1	26, 27, 28, 35, 36	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2 - COSO Principle 11		

bernard@...otmaker.io

Google Confidental Information

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC5.2	26, 27, 28, 36, 37, 38, 39, 40, 41	The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3 - COSO Principle 12		
CC5.3	19, 33, 34, 39, 42, 43	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.1		
CC6.1	31, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2		
CC6.2	40, 41, 54, 55, 56, 65, 66, 67, 68	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3		
CC6.3	40, 41, 65, 66, 67	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
CC6.4		
CC6.4	69, 70, 71, 72, 73, 74, 75, 76, 77	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

bernard@botmaker.io

Google Confidental Information

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC6.5		
CC6.5	78	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6		
CC6.6	41, 57, 58, 59, 79, 80, 81	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7		
CC6.7	59, 60, 77, 81, 82, 83, 84, 85, 86, 87, 88, 89	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8		
CC6.8	30, 90, 91, 92, 93	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
CC7.1		
CC7.1	30, 87, 92, 94, 95, 96, 97	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2		
CC7.2	27, 30, 93, 97, 98, 99, 100	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

bernal@bowmaker.io

Google Confidental Information

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC7.3		
CC7.3	20, 92, 93, 97, 99, 100, 101, 102, 103	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
CC7.4		
CC7.4	93, 97, 99, 100, 101, 102, 103, 104	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5		
CC7.5	43, 93, 97, 99, 105	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.1		
CC8.1	15, 61, 88, 93, 106, 107, 108, 109, 110	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.1		
CC9.1	111, 112, 113, 114	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2		
CC9.2	5, 115, 116, 117, 118, 119, 120, 121, 122	The entity assesses and manages risks associated with vendors and business partners.

bernardo@bonmaker.io

Google Confidental Information

Criteria to Controls Mapping

Criteria	Controls List	Criteria
A1.1		
A1.1	68, 92, 93, 104	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2		
A1.2	68, 104, 112, 113, 114, 123, 124	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.
A1.3		
A1.3	27, 28, 99, 104, 112, 113, 114	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
C1.1		
C1.1	5, 24, 62, 63, 64, 100, 117, 118, 119, 120, 121, 125, 126	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2		
C1.2	62, 63, 127	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
P1.1		
P1.1	127, 128, 129	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.

bernard@bormaker.co

Google Confidental Information

Criteria to Controls Mapping

Criteria	Controls List	Criteria
P2.1		
P2.1	127, 128	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.
P3.1		
P3.1	126, 128, 129	Personal information is collected consistent with the entity's objectives related to privacy.
P3.2		
P3.2	128	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.
P4.1		
P4.1	64, 128, 129	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.
P4.2		
P4.2	62, 63, 127, 128	The entity retains personal information consistent with the entity's objectives related to privacy.
P4.3		
P4.3	62, 63, 78, 89, 127	The entity securely disposes of personal information to meet the entity's objectives related to privacy.

bernard@bottmaker.io

Criteria to Controls Mapping

Criteria	Controls List	Criteria
P5.1		
P5.1	130, 131, 132	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.
P5.2		
P5.2	130, 131, 132	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.
P6.1		
P6.1	121, 122, 133, 134, 135	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.
P6.2		
P6.2	136	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.
P6.3		
P6.3	99, 101, 102, 103, 137	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.
P6.4		
P6.4	121, 122, 133, 134	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.

bernal@bonadio.io

Criteria to Controls Mapping

Criteria	Controls List	Criteria
P6.5		
P6.5	121, 137	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.
P6.6		
P6.6	103, 121	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.
P6.7		
P6.7	132, 135, 138	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.
P7.1		
P7.1	128, 132	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.
P8.1		
P8.1	139, 140, 141, 142	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.

bernard@ostmalta.io

SECTION V - Other Information Provided by Google LLC

bernard@botmaker.io

Google Confidental Information

Google

Other Information Provided by Google LLC

Internal Google Traffic

Connections between internal Google resources use proprietary services similar to Remote Procedural Calls (RPC) that provide peer-to-peer authentication similar to Kerberos. All traffic is at least cryptographically authenticated between machines, while some connections, including to and from the Key Management Service, are encrypted using AES.

Key Management

Google uses a proprietary service to manage the distribution, generation and rotation of cryptographic keys. Files or data structures with user-generated content written by Cloud or App Engine services are encrypted with a key. This key is encrypted by the Key Management Service with a restricted access control list (ACL) of services allowed to request the Key Management Service to decrypt it. The encrypted key is not stored alongside the encrypted data.

The wrapping keys needed to decrypt user data are only known to the Key Management Service. All access to/from the Key Management Service is controlled by ACLs. Access is restricted to a limited number of individuals and applications, and auditing is enabled to determine whether access is appropriate.

Key Rotations

Google uses a proprietary system to periodically generate and rotate an encryption key used to protect user data at rest on average at least every 90 days. New wrapped encryption keys are generated for each new Google storage file (a Google file is defined in Encryption of Data Stored at Google above). The system helps ensure that key rotations are managed appropriately, and that customer data is not encrypted with a discarded key.

Disk Erase Process

Google has a policy stating that no loose drive may leave Google data centers unless it has been erased (or destroyed), certified as erased by Google, and validated as such by Google via audit. One or more types of disk erase mechanisms are used to delete data off disks before they are decommissioned. Multiple checks are performed to help ensure that all drives are accounted for. Non-erased loose drives are stored in a secure container until they are erased. The disk erase process is well defined, and each facility is audited on a daily basis to monitor compliance with the disk erase policy.

If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

bernard@botmaker.io

Google Confidental Information

Gemini 3 Pro Model Documentation

The EU AI Act requires providers of general-purpose AI models to provide information and documentation to downstream providers that integrate or intend to integrate the model into their AI system.

Please refer to the relevant terms of service to determine which Google entity is the service provider. For the European Economic Area, the model provider is Google Ireland Limited.

The total number of parameters of Gemini 3 Pro is over 1 trillion. For more model information and documentation, see the Model Information, Model Data, Distribution, and Intended Usage and Limitations sections of the Model Card and also the API documentation.

bernard@botmaker.io

PLANILHA DE ORÇAMENTO – PROCESSO Nº 0000862.2024

OBJETO: Serviços de subscrição de Software como serviço (SaaS – Software as a Service) que permita o atendimento por agentes virtuais ou humanos, por meio do aplicativo de mensagens instantâneas Whatsapp, do Grupo Meta, conforme condições e requisitos do edital e seus anexos.

1. **DEMAIS CONDIÇÕES:** Conforme Termo de Referência do processo.

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE ESTIMADA	VALOR UNITÁRIO (R$)	VALOR MENSAL (R$)	VALOR TOTAL 60 MESES (R$)
1	**Setup da solução**					
1.1	Instalação e configuração	Un	1	41.119,00	41.119,00	41.119,00
1.2	Implementação dos serviços	Un	1	106.150,00	106.150,00	106.150,00
					Valor total item 1	147.269,00
2	Treinamento	Hora/aula	320	R$ 108,43	-----	34.696,00
					Valor total item 2	34.696,00
3	**Licenças p/Agente de Atendimento/Supervisor**					
3.1	Por agente de atendimento (DE 4.001 até 5.000)	Licença por usuário identificado/mês	3.421	19,00	64.999,000	3.899.940,00
3.2	Por agente de atendimento + Supervisão (DE 500 até 1000)		629	19,00	11.951,00	717.060,00
					Valor total item 3	4.617.000,00
4	**Custo plataforma (Montly Active Users) MAU**	Contatos únicos/ mês	760.000	0,16	122.189,57	7.331.374,00
					Valor total item 4	7.331.374,00
5	**Mensagens WhatsApp de resposta aos clientes**					
5.1	Marketing	Conversas/mês	0	0,45	0,00	0,00
5.2	Utility		616.850	0,00	0,00	0,00
5.3	Authentication		3.150	0,05	157,50	9.450,00
5.4	Service		310.000	0,00	0,00	0,00

Clicksign 02d60e37-58c7-431a-8657-4b85ea597d0a

					Valor total item 5	9.450,00
6	**Mensagens WhatsApp iniciadas pelo Banco**					
6.1	Marketing (CENTRALIZADO)	Conversas/mês	780.000	0,45	351.000,00	21.060.000,00
6.2	Marketing (REDE AGS)		250.515	0,45	112.731,75	6.763.905,00
6.3	Utility		620.000	0,05	31.000,00	1.860.000,00
6.4	Authentication		0	0,05	0,00	0,00
					Valor total item 6	29.683.905,00
7	**Consultoria de melhoria contínua**	Hora	10.000	250,00	-----	2.500.000,00
					Valor total item 7	2.500.000,00
				VALOR TOTAL		**44.323.694,00**

2. OBSERVAÇÃO

As quantidades dos itens “Mensagens” estão mensuradas em conversas dia (janela de 24 horas)

3. REGRAMENTO DE PRECIFICAÇÃO:

Nos preços propostos e naqueles que, porventura, vierem a ser ofertados através de lances, deverão estar inclusos todos os custos necessários à execução do objeto, bem como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros e quaisquer outros que incidam ou venham incidir sobre o mesmo.

4. DADOS DA PROPONENTE:

RAZÃO SOCIAL - BM Brasil Internet Ltda
CNPJ - 30.607.960/0001-85
ENDEREÇO COMPLETO - Rua Surubim, 577, Conjuntos 171 e 172, 17º andar – Cidade Monções – São Paulo/SP – CEP 04571-050
TELEFONE - 11 97091-2608
E-MAIL - fernando.dionizio@botmaker.io
DADOS BANCÁRIOS -

- **Código do Banco - 341**
- **Nº da Agência - 0393**
- **Nº da Conta Corrente PJ - 29949-0**

Clicksign 02d60e37-58c7-431a-8657-4b85ea597d0a

5. VALIDADE DA PROPOSTA: 27 de Fevereiro de 2026

Por ser expressão da verdade, firmamos a presente declaração.

SÃO PAULO, 27 de Novembro de 2025

Fernando Nascimento Dionizio

Sr Sales Executive

BM BRASIL INTERNET LTDA

CNPJ nº 30.607.960/0001-85

Clicksign 02d60e37-58c7-431a-8657-4b85ea597d0a

PLANILHA DE ORÇAMENTO – PROCESSO Nº 0000862.2024 - BM BRASIL INTERNET V.2.pdf

Documento número #02d60e37-58c7-431a-8657-4b85ea597d0a

Hash do documento original (SHA256): cba0ce413d7ce7c2392275ee46f5b328eb4d30f79fb3346c9bfaebe435224281

Assinaturas

Fernando Nascimento Dionizio
CPF: 357.704.108-09
Assinou em 27 nov 2025 às 16:23:22

Log

27 nov 2025, 16:22:58	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 criou este documento número 02d60e37-58c7-431a-8657-4b85ea597d0a. Data limite para assinatura do documento: 27 de dezembro de 2025 (16:22). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
27 nov 2025, 16:23:20	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 alterou o processo de assinatura. Data limite para assinatura do documento: 28 de novembro de 2025 (16:37).
27 nov 2025, 16:23:20	Operador com email fernando.dionizio@botmaker.com na Conta 8cb3ad58-67cc-4c35-806a-692ffe11ba97 adicionou à Lista de Assinatura: fernando.dionizio@botmaker.com para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Fernando Nascimento Dionizio e CPF 357.704.108-09.
27 nov 2025, 16:23:22	Fernando Nascimento Dionizio assinou. Pontos de autenticação: Token via E-mail fernando.dionizio@botmaker.com. CPF informado: 357.704.108-09. IP: 187.90.244.150. Componente de assinatura versão 1.1352.1 disponibilizado em https://app.clicksign.com.
27 nov 2025, 16:23:22	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 02d60e37-58c7-431a-8657-4b85ea597d0a.

ICP Brasil

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 02d60e37-58c7-431a-8657-4b85ea597d0a, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.