



**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, 2023 to
March 31, 2024**



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, 2023 to March 31, 2024..... 10

Section 4

Presentation of Objectives, Basic Criteria, Assigned Controls, Service Auditor's
Tests and Results of Tests 56

Section 5

Other Information Provided by Google LLC..... 287

support@cora.cloud

Section 1

Independent Service Auditor's Report

support@cora.cloud

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, 2023 to March 31, 2024" (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, 2023 to March 31, 2024. 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, 2023 to March 31, 2024, 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, 2023 to March 31, 2024. 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.

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 risk 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 have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. Our engagement team included members with Certified Information Systems Auditor and Cloud Security Alliance Certificate of Cloud Security Knowledge certifications.

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 change 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, 2023 to March 31, 2024 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, 2023 to March 31, 2024, 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, 2023 to March 31, 2024, 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 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 6, 2024

support@cora.cloud

Section 2

Assertion of Google LLC Management

support@corp.cloud



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)

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, 2023 to March 31, 2024 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, 2023 to March 31, 2024, if the subservice organizations and user entities applied the complementary controls assumed in the design of Google’s controls throughout that period; and

Google Confidential Information

- The controls stated in the description were suitably designed and operated effectively throughout the period April 1, 2023 to March 31, 2024, 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

support@cora.cloud

Section 3

Description of the Internal Control System Related to Google LLC's Google Cloud Platform Throughout the Period April 1, 2023 to March 31, 2024

support@corecloud

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 this 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 pre-trained 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
- Internet of Things (IoT): Scalable, fully managed IoT cloud services to connect, process, store, and analyze data at the edge and in the cloud
- 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

Google Confidential Information

- 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: 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; 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:

- AI and ML
 - Agent Assist¹
 - AI Platform Deep Learning Container
 - AI Platform Neural Architecture Search (NAS)
 - AI Platform Training and Prediction
 - Anti-Money Laundering (AML) AI¹
 - AutoML Natural Language
 - AutoML Tables
 - AutoML Translation
 - AutoML Video
 - AutoML Vision
 - Cloud Natural Language API
 - Cloud Speaker ID
 - Cloud Translation
 - Cloud Vision
 - Contact Center AI (CCAI)
 - Contact Center AI Insights
 - Contact Center AI Platform
 - Dialogflow
 - Discovery Solutions
 - Document AI
 - Document AI Warehouse

¹Indicates products in scope only for the period May 1, 2023 through October 31, 2023.

- Gemini for Google Cloud
- Generative AI on Vertex AI (formerly Generative AI Support on Vertex AI)¹
- Recommendations AI
- Retail Search
- Speech-to-Text
- Talent Solution
- Text-to-Speech
- Vertex AI Codey
- Vertex AI Colab Enterprise
- Vertex AI Conversation (formerly Generative AI App Builder)¹
- Vertex AI Data Labeling
- Vertex AI Platform (formerly Vertex AI)
- Vertex AI Search (formerly Gen App Builder – Enterprise Search)¹
- Vertex AI Workbench Instances
- Video Intelligence API
- 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 (formerly Google Genomics)
 - Data Catalog
 - Dataflow
 - Dataform
 - Dataplex
 - Dataproc

- Dataproc Metastore
- Looker Studio (formerly Google Data Studio)
- 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
- IoT
 - IoT Core

- Management Tools
 - Cloud Console
 - Cloud Console App
 - Cloud Deployment Manager
 - Cloud Shell
 - Recommender
 - Service Infrastructure
- Media and Gaming
 - Game Servers²
 - 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 Firewall
 - Cloud IDS (Cloud Intrusion Detection System)
 - Cloud Interconnect
 - Cloud Load Balancing
 - Cloud Network Address Translation (NAT)
 - 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

²Game Servers was deprecated on June 30, 2023.

- Traffic Director
- Virtual Private Cloud (VPC)
- Operations
 - Cloud Debugger
 - Cloud Logging
 - Cloud Monitoring
 - Cloud Profiler
 - Cloud Trace
- Security and Identity
 - Access Approval
 - Access Context Manager
 - Access Transparency
 - Assured Workloads
 - BeyondCorp Enterprise
 - Binary Authorization
 - Certificate Authority Service
 - Certificate Manager
 - Cloud Asset Inventory
 - Cloud External Key Manager (Cloud EKM)
 - Cloud HSM
 - Cloud Key Management Service
 - Firebase App Check
 - Firebase Authentication
 - Google Cloud Identity-Aware Proxy
 - Identity and Access Management (IAM)
 - Identity Platform
 - Key Access Justifications (KAJ)
 - Managed Service for Microsoft Active Directory (AD)
 - reCAPTCHA Enterprise
 - Resource Manager API
 - Risk Manager
 - 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
 - Persistent Disk
- Other
 - Chronicle SIEM³
 - Google Cloud Threat Intelligence for Chronicle³
 - Cloud Billing
 - Google Earth Engine
 - Google Cloud Marketplace
 - Tables

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.

³Chronicle SIEM and Threat Intelligence for Chronicle are covered by separate terms than GCP. Refer to the Terms of Service (<https://chronicle.security/legal/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 Google Kubernetes Engine (GKE), Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.

AI Platform Neural Architecture Search (NAS)

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 (AML) 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 Natural Language

AutoML Natural Language enables customers to categorize input text into their own custom-defined labels (supervised classification). Users can customize models to their own domain or use case.

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 (GNMT) model for their own domain or use-case.

AutoML Video

AutoML Video delivers a simple and flexible ML service that lets businesses and customer developers train custom and scalable video models for specific domains or use cases.

AutoML Vision

AutoML Vision is a simple and flexible ML service that lets businesses and developers with limited ML expertise train custom and scalable vision models for their own use cases.

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.

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.

Contact Center AI (CCAI)

CCAI is a solution for improving the customer experience in user contact centers using AI. CCAI encompasses Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Speech-to-Text, and Text-to-Speech.

Contact Center AI Insights

Contact Center AI Insights is aimed at contact centers. It features virtual agent and agent assist, which improve the contact center experience during conversations. After completion, conversations can be analyzed with AI models and algorithms to present valuable metrics to customers.

Contact Center AI Platform

Contact Center AI Platform is an AI-driven contact-center-as-a-service (CCaaS) platform built natively on Google Cloud, leveraging Contact Center AI at its core. CCAI Platform is built to work alongside customer relationship management (CRM) systems and accelerates the organization's ability to leverage and deploy AI-driven contact center functionalities. CCAI Platform is a full-stack contact center platform for queuing and routing customer interactions across voice and digital channels. It provides easy routing of customer interactions to the appropriate resource pools, allowing a seamless transition to human agents.

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.

Gemini for Google Cloud (Formally known as Duet AI 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.

Generative AI on Vertex AI (formerly Generative AI Support 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.

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 (ATSs), 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 (formerly Generative AI App Builder)

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

Vertex AI Data Labeling

Vertex AI Data Labeling is a service that helps developers obtain data to train and evaluate their machine learning models. It supports labeling for image, video, text, and audio as well as centralized management of labeled data.

Vertex AI Platform (formerly Vertex AI)

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 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 (formerly Gen App Builder – Enterprise 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 acts as your 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 you for further action. Additionally, it evaluates your API setups against security best practices, offering recommendations for improvement. This comprehensive approach helps you proactively safeguard your APIs, protect sensitive data, and ensure your 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.

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 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.

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 a metadata storage service component for data lakes built on open-source processing frameworks (e.g., Apache Hadoop, Apache Spark, Apache Hive, Presto).

Looker Studio (formerly Google Data 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.

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.

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 Remote Dictionary Server (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 Google Kubernetes Engine (GKE) for quick enablement. The service works with both Google Cloud's first-party products and also lets you 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.

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 Infra Manager, enabling you 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 (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, powered by the open-source container scheduler Kubernetes, runs containers on GCP. Google Kubernetes Engine manages provisioning and maintaining the underlying VM 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 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.

Internet of Things

IoT Core

IoT Core is a fully managed service that securely connects, manages, and ingests data from Internet-connected devices. It enables utilization of other GCP services for collecting, processing, and analyzing IoT data.

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.

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

Game Servers

Game Servers is a managed service that enables game developers to deploy and manage their dedicated game servers across multiple Agones clusters, dedicated game servers built on Kubernetes, around the world through a single interface.

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 (formerly Migrate for Compute Engine)

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.

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 Firewall

Cloud Firewall 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-premise networks and GCP VPC.

Cloud Load Balancing

Cloud Load Balancing is a distributed, software-defined, managed service for all traffic (HTTP(S), 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.

Cloud VPN

Cloud VPN provides connections between on-premises or other external networks to virtual private clouds 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 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 GCP's traffic management service for open-source service meshes.

Virtual Private Cloud (VPC)

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

Operations

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 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.

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).

BeyondCorp Enterprise

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

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 (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.

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 (EKM)

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 (HSM)

Cloud HSM is a cloud-hosted, hardware security module 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.

Firestore App Check

Firestore 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.

Firestore Authentication

Firestore 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.

Google Cloud Identity-Aware Proxy (IAP)

Google Cloud IAP is a tool that helps control access to applications running on GCP based on identity and group membership.

Identity and Access Management (IAM)

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)

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.

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.

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 or DLP)

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.

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 (or Google Kubernetes Engine) 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 VM instances or Google Kubernetes Engine 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.

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 and hard disk drive (HDD) variations.

Other

Chronicle SIEM

Chronicle 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 Cloud Threat Intelligence (GCTI) or Threat Intelligence for Chronicle

GCTI is a service extension for Chronicle 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 special review or logs that should be automatically sent to customers.

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.

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 (PoPs).

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.

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 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 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.

Google Confidential Information

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 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.

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.

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 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

Google Confidential Information

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 are 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.

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).

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.

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 electronic mail 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 Confidential Information

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.

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 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

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.

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.

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).

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

Google Confidential Information

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 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 on a semiannual basis 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 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, 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 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

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 place.
- 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.
- 24x7 on-site security personnel are in place.

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.

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, uninterrupted power supply (UPS), generators, HVAC, and emergency lighting systems. Please refer to the Types of Services section above for a list of Google's data center locations.

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.

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 a continuous basis 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 6 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.

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.

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 notifying 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
- 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.

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.

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, central processing unit 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.

Disaster Recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, 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

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.

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 its 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 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.

Google Confidential Information

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.
- 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.

Google Confidential Information

- 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.
- 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.
 - 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.
- 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.

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, 2023 to March 31, 2024.

The Applicable Cloud Computing Compliance Criteria Catalogue 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.

No.	Area (identifier)	Objective
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.
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.

Google’s applicable controls supporting the C5 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.

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 agreement, stay informed of changes planned at the hosting facility, 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-03, PS-04, PS-05, PS-06	All third party colocation providers have some responsibility for preventing unauthorized physical access and protecting against theft, damage, and outage of operations. Specific monitoring controls performed by the Company relative to these CSOCs are described in Section 4 of this report.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the GCP was used to provide the service from April 1, 2023 to March 31, 2024.

Report Use

The description does not omit or distort information relevant to the 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.

Section 4

Presentation of Objectives, Basic Criteria, Assigned Controls, Service Auditor's Tests and Results of Tests

support@calfire-cloud

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: <ul style="list-style-type: none"> • 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 required to be 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 were in accordance 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.

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
<p>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.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
<p>Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.</p>	<p>Inspected the organization's security and privacy policies on the intranet to determine that they 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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>

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
<p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>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.</p>	<p>Inspected the Cloud Data Processing Addendum (CDPA) template to determine that the organization required external parties (Service Providers) to meet security & privacy requirements for safeguarding user data and that requirements were enforced via the "Information Protection Addendum (IPA)" or the "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.</p>	<p>No exceptions noted.</p>
	<p>Inspected the Inbound Service Agreement (ISA) and the Subprocessor Data Processing Agreement (SDPA) for a sample of processors and sub-processors supporting the in-scope systems to determine that the organization had implemented an addendum to contract with processors and sub-processors.</p>	<p>No exceptions noted.</p>
	<p>Inspected the termination clause for service issues related to vendors within an example ISA and an example SPDA 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.</p>	<p>No exceptions noted.</p>

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 Security Engineering Org had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
	Inspected the VSA review documentation, Quarterly Business Reports, and Monthly Business Reports for a sample of vendors to determine that the reviews included automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	No exceptions noted.
The organization requires subprocessors to meet security & 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 where Google was a processor, with requirements being 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 were in accordance 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.

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
<p>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.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
<p>Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.</p>	<p>Inspected the organization's security and privacy policies on the intranet to determine that they 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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>

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
<p>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:</p> <ul style="list-style-type: none"> • Vulnerabilities; • Security incidents; and • Malfunctions. <p>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.</p>		
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.
	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 ToS to determine that the organization's commitments to security, availability, processing integrity, 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, processing integrity, and confidentiality were communicated to external users via publications.	No exceptions noted.

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 to customer-facing services that could have affected security, confidentiality, processing integrity, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker webpage, 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, processing integrity, 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 Google Cloud Platform 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.

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 used for the compliance with legal and regulatory requirements defined in the Data Security Policy, the Data Classification Guidelines and procedures, and the Code of Conduct to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.
	Inspected the organizational and technical safeguards the Company used for the protection of data, IT applications, and IT infrastructure within 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 Cloud Data Processing Addendum (CDPA) template to determine that the organization required external parties (Service Providers) to meet security & privacy requirements for safeguarding user data and that requirements were enforced via the "Information Protection Addendum (IPA)" or the "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	No exceptions noted.

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 Inbound Service Agreement (ISA) and the Subprocessor Data Processing Agreement (SDPA) for a sample of processors and sub-processors supporting the in-scope systems to determine that the organization had implemented an addendum to contract with processors and sub-processors.	No exceptions noted.
	Inspected the termination clause for service issues related to vendors within an example ISA and an example SPDA 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.
<p>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:</p> <p>Administration of rights profiles, approval and assignment of access and access authorizations (cf. IDM-01);</p> <ul style="list-style-type: none"> • Development, testing, and release of changes (cf. DEV-01); and • Operation of the system components. <p>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.</p>		
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.

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
<p>The organization conducts Information Security Risk Assessments at least annually to identify and evaluate risks.</p>	<p>Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment to identify and evaluate risks.</p>	<p>No exceptions noted.</p>
	<p>Inspected the risk assessment and the Internal Access Control program documents 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.</p>	<p>No exceptions noted.</p>
	<p>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:</p> <ul style="list-style-type: none"> - Administration of rights profiles, approval and assignment of access, and access authorizations - Development, testing, and release of changes - Operation of the system components 	<p>No exceptions noted.</p>
	<p>Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas:</p> <ul style="list-style-type: none"> - 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 	<p>No exceptions noted.</p>

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 Account Security Policy and the Identity and Access Management Policy to determine that the organization separated duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	No exceptions noted.
	Observed an attempt to access a privileged system outside the realm of the user's job responsibilities to determine that the attempt to violate the separation of duties failed and that the organization separated duties and implemented a principle of least privilege by limiting access to only authorized users.	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 example new hire and transferred employees to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.

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 systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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 a version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected the annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to the version control system was required to be approved.	No exceptions noted.
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 Company websites on the intranet to determine that the organization was an active participant in the security industry and maintained appropriate contacts with special interest groups, security forums, and professional associations.	No exceptions noted.
	Inspected the Google security overview external-facing webpage 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.

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 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 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.
	Inspected 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 within the Company.	No exceptions noted.
<p>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:</p> <ul style="list-style-type: none"> • 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.

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
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 they 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.

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
<p>OIS-07: Application of the Risk Management Policy</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>		
<p>The organization conducts Information Security Risk Assessments at least annually to identify and evaluate risks.</p>	<p>Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment to identify and evaluate risks.</p>	<p>No exceptions noted.</p>
	<p>Inspected the risk assessment and the Internal Access Control program documents 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.</p>	<p>No exceptions noted.</p>
	<p>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:</p> <ul style="list-style-type: none"> - Administration of rights profiles, approval and assignment of access, and access authorizations - Development, testing, and release of changes - Operation of the system components 	<p>No exceptions noted.</p>

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
	<p>Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas:</p> <ul style="list-style-type: none"> - 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.
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 Account Security Policy and the Identity and Access Management Policy to determine that the organization separated duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	No exceptions noted.
	Observed an attempt to access a privileged system outside the realm of the user's job responsibilities to determine that the attempt to violate the separation of duties failed and that the organization separated duties and implemented a principle of least privilege by limiting access to only authorized users.	No exceptions noted.

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 conducts Information Security Risk Assessments at least annually 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 to identify and evaluate risks.	No exceptions noted.
	Inspected the risk assessment and the Internal Access Control program documents 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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.

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 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.

support@cora.com

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
<p>SP-01: Documentation, Communication and Provision of Policies and Instructions</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>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.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
<p>The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.</p>	<p>Inspected the organization's security policies and procedures to determine that they addressed security, confidentiality, and availability; had been approved by management; and were in accordance with ISO 27001.</p>	<p>No exceptions noted.</p>

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 they 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.

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.
<p>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:</p> <ul style="list-style-type: none"> • Organizational and technical changes in the procedures for providing the cloud service; and • Legal and regulatory changes in the Cloud Service Provider's environment. <p>Revised policies and instructions are approved before they become effective.</p>		
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 they 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.

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 webpage 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's approvals for policy exceptions 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.

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
<p>HR-01: Verification of Qualification and Trustworthiness</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>Background checks are performed on new hires as permitted by local laws.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
<p>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.</p>	<p>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.</p>	<p>No exceptions noted.</p>

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
<p>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.</p>		
<p>The organization has established a code of conduct that is reviewed and updated as needed.</p>	<p>Inspected the Code of Conduct, Basic Internal Privacy Policy, Information Security 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 are reviewed and updated as needed.</p>	<p>No exceptions noted.</p>
<p>Personnel of the organization are required to acknowledge the code of conduct.</p>	<p>Inspected acknowledgements of the Code of Conduct and information security policies for a sample of new hires, 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.</p>	<p>No exceptions noted.</p>
<p>The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.</p>	<p>Inspected extended workforce personnel responsibilities and expected behavior for the protection of information within the confidentiality agreement template to determine that the organization established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.</p>	<p>No exceptions noted.</p>

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 that 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.
<p>HR-03: Security Training and Awareness Program</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		

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
<p>The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.</p>	<p>Inspected the internal Privacy Policy, Basic Security Policy, privacy and information security training program materials, and compliance monitoring tools to determine that a privacy and information security training program was established and that relevant personnel were required to complete this training annually.</p>	<p>No exceptions noted.</p>
	<p>Inspected the compliance monitoring tool dashboard used by management to monitor the completion rate for employees' completion of the required privacy and information security training, as well as configurations for the automated training enrollment tool, and an example of an email notification sent to employees for overdue training to determine that the organization had established a privacy and information security training program and that relevant personnel met the requirement to complete the training annually.</p>	<p>No exceptions noted.</p>
	<p>Inspected the security awareness training content to determine that security awareness training content was reviewed and updated at least annually.</p>	<p>No exceptions noted.</p>

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.

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 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 "Leaving the Company" website for termination procedures to determine that the organization established and communicated personnel offboarding procedures that governed the removal of access and return of assets and that, as part of the offboarding process, terminated employees and Temps, Vendors, and Contractors (TVCs) were required to return Google property and assets that they were assigned or given during their employment at Google.	No exceptions noted.
	Inspected the internal "Leaving the Company" website 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 area of responsibility changed or their employment relationship was terminated.	No exceptions noted.

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 terminated employee Exit Certification Letter template to determine that all organizational assets in their possession were requested and required to be returned upon termination from the Company, 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, Information Security 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 are 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 hires, 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 extended workforce personnel responsibilities and expected behavior for the protection of information within the confidentiality agreement template to determine that the organization established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	No exceptions noted.

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 that 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-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.

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
<p>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.</p> <p>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 would require an acknowledgement of the updated versions.</p>	<p>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 these confidentiality agreements and information sharing agreements were reviewed annually.</p>	<p>No exceptions noted.</p>
	<p>Inquired of 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 warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether any changes made to confidentiality agreements as a result of the annual review required acknowledgements of the updated versions.</p>	<p>Not tested. No changes were made to confidentiality agreements during the period that would require an acknowledgement of the updated versions.</p>
<p>The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.</p>	<p>Inspected extended workforce personnel responsibilities and expected behavior for the protection of information within the confidentiality agreement template to determine that the organization established confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.</p>	<p>No exceptions noted.</p>
	<p>Inspected confidentiality agreement acknowledgements for a sample of extended workforce personnel to determine that extended workforce personnel acknowledged the organization's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information.</p>	<p>No exceptions noted.</p>

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
<p>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.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
<p>The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>

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
<p>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.</p>		
<p>Automated mechanisms are utilized to track inventory of all production machines and inventory of all serialized server components.</p>	<p>Inspected the Device Configuration Guidelines to determine that the organization established procedures around the automated mechanisms that were utilized to track inventory of production machines.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>

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 Google Cloud Platform 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 governing security of corporate-managed devices providing privileged access.	No exceptions noted.
	Inspected the configurations for the software management systems to install software and track usage to determine that the organization had established mechanisms governing the configuration of corporate-managed devices providing privileged access.	No exceptions noted.
The organization maintains an up-to-date, accurate client device inventory	Inspected the procedures for inventorying client assets and an example of the client asset inventory review performed to determine that the organization maintained an updated, completed, accurate, valid, 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 used for the compliance with legal and regulatory requirements defined in the Data Security Policy, the Data Classification Guidelines and procedures, and the Code of Conduct to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.

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 the Company used for the protection of data, IT applications, and IT infrastructure within 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.
<p>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:</p> <ul style="list-style-type: none"> • 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 and Source Code Guidelines to determine that the organization had developed policies, procedures, and guidelines governing the secure development lifecycle.	No exceptions noted.

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 Requirements for Outsourced Software Development Policy to determine that outsourced development was required to be controlled according to requirements set forth in policies relevant to system development and acquisition and that applications were required to be tested and analyzed for vulnerabilities prior to acceptance.	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 information according to 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 Guidelines regarding encryption mechanisms to determine that the organization required the use of encryption to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
	Inspected the CDPA website made available to external users regarding encryption mechanisms to determine that the organization communicated to external users on how user authentication and administrator sessions transmitted over the internet were encrypted.	No exceptions noted.
	Inspected server scan results and configurations around encryption mechanisms to determine that the organization used encryption mechanisms to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.

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
	Observed a user and an administrator's connection settings to the organization's external websites to determine that encryption was 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 documented key management process within the organization's Cryptographic Guidelines to determine that the organization had an established key management process in place to support the organization's use of cryptographic techniques.	No exceptions noted.
	Inspected the code configuration enforcing encryption and certificate authentication and revocation to determine that the organization had an established key management process in place to support 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 SDLC policy and software management systems to determine that the Company had policies and procedures in place that governed the use of intellectual property and third-party software and that the organization 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 network and systems.	No exceptions noted.

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 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 technical and organizational safeguards for the secure handling of metadata within the Data Security Policy to determine that the organization had security policies that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.	No exceptions noted.
	Inspected guidance and security policies related to metadata handled by product teams to determine that the organization had implemented security processes that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.	No exceptions noted.
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the Network Device and Configuration Guidelines to determine that the Company hardened virtual environments where the organization had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected the configuration of the tool used to enforce a standard production image for the installation and maintenance of Company servers to determine that the organization hardened virtual environments where it had a responsibility as outlined in the shared responsibilities.	No exceptions noted.

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 customer image restriction functionality within the cloud portal and the default hardening standards for virtual machines and containers to determine that customers were provided mechanisms for the restriction of the available selections of default hardened images for virtual machines and containers to be used within their 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, Information Security 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 are 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 extended workforce personnel responsibilities and expected behavior for the protection of information within the confidentiality agreement template to determine that the organization 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 that defined responsibilities and expected behavior for the protection of information.	No exceptions noted.

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 policies and guidelines that govern the acceptable use of information assets.	Inspected the defined goals, roles, responsibilities, department coordination requirements, and the safeguards used for the compliance with legal and regulatory requirements defined in the Data Security Policy, the Data Classification Guidelines and procedures, and the Code of Conduct to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.
	Inspected the organizational and technical safeguards the Company used for the protection of data, IT applications, and IT infrastructure within 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 they 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.

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 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 governing security of corporate-managed devices providing privileged access.	No exceptions noted.
	Inspected the configurations for the software management systems to install software and track usage to determine that the organization had established mechanisms governing the configuration of corporate-managed devices providing 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 before being deployed.	No exceptions noted.

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
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 example new hire and transferred employees to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the Network Device and Configuration Guidelines to determine that the Company hardened virtual environments where the organization had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected the configuration of the tool used to enforce a standard production image for the installation and maintenance of Company servers to determine that the organization hardened virtual environments where it had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected customer image restriction functionality within the cloud portal and the default hardening standards for virtual machines and containers to determine that customers were provided mechanisms for the restriction of the available selections of default hardened images for virtual machines and containers to be used within their cloud environment.	No exceptions noted.

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 policies and guidelines governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy and Source Code Guidelines to determine that the organization had developed policies, procedures, and guidelines governing the secure development lifecycle.	No exceptions noted.
	Inspected Security Requirements for Outsourced Software Development Policy to determine that outsourced development was required to be controlled according to requirements set forth in policies relevant to system development and acquisition and that applications were required to be tested and analyzed for vulnerabilities prior to acceptance.	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 around the 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.

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.
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 information according to 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.
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 the Data Destruction Guidelines to determine that the organization was required to sanitize storage media prior to disposal, release from organizational control, or release for reuse.	No exceptions noted.

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
	Performed remote inspections for a sample of data centers to determine that the organization sanitized storage media prior to 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 the asset management guidelines 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 deactivation process and configurations to determine that the organization had mechanisms in place that prevented 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' code configuration that assigned reviews to the authorized group administrators to determine that critical access groups were reviewed at least annually.	No exceptions noted.
	Inspected critical access group user membership reviews performed by group administrators for a sample of products 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.
	Inspected automatic account revocation configurations to determine that inappropriate access identified as a result of the semi-annual critical access group membership reviews was removed at least hourly.	No exceptions noted.

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 established a code of conduct that is reviewed and updated as needed.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Information Security 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 are 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 extended workforce personnel responsibilities and expected behavior for the protection of information within the confidentiality agreement template to determine that the organization 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 that 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.

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 established an offboarding procedure for personnel, which governs the removal of access and return of assets.	Inspected the internal "Leaving the Company" website for termination procedures to determine that the organization established and communicated personnel offboarding procedures that governed the removal of access and return of assets and that, as part of the offboarding process, terminated employees and Temps, Vendors, and Contractors (TVCs) were required to return Google property and assets that they were assigned or given during their employment at Google.	No exceptions noted.
	Inspected the internal "Leaving the Company" website 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 area of responsibility changed or their employment relationship was terminated.	No exceptions noted.
	Inspected the terminated employee Exit Certification Letter template to determine that all organizational assets in their possession were requested and required to be returned upon termination from the Company, 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 used for the compliance with legal and regulatory requirements defined in the Data Security Policy, the Data Classification Guidelines and procedures, and the Code of Conduct to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.

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 the Company used for the protection of data, IT applications, and IT infrastructure within 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 governing security of corporate-managed devices providing privileged access.	No exceptions noted.
	Inspected the configurations for the software management systems to install software and track usage to determine that the organization had established mechanisms governing the configuration of corporate-managed devices providing 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 & 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.

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 root cause analysis and remediation documentation for a sample of security event tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, 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 to determine whether they could have resulted in a failure to meet 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 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.

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 technical and organizational safeguards for the secure handling of metadata within the Data Security Policy to determine that the organization had security policies that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.	No exceptions noted.
	Inspected guidance and security policies related to metadata handled by product teams to determine that the organization had implemented security processes that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.	No exceptions noted.
The organization maintains an up-to-date, accurate client device inventory	Inspected the procedures for inventorying client assets and an example of the client asset inventory review performed to determine that the organization maintained an updated, completed, accurate, valid, and consistent client device inventory throughout the asset lifecycle.	No exceptions noted.
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the Network Device and Configuration Guidelines to determine that the Company hardened virtual environments where the organization had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected the configuration of the tool used to enforce a standard production image for the installation and maintenance of Company servers to determine that the organization hardened virtual environments where it had a responsibility as outlined in the shared responsibilities.	No exceptions noted.

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 customer image restriction functionality within the cloud portal and the default hardening standards for virtual machines and containers to determine that customers were provided mechanisms for the restriction of the available selections of default hardened images for virtual machines and containers to be used within their 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 around the 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.

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
<p>PS-01: Physical Security and Environmental Control Requirements</p> <p>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:</p> <ul style="list-style-type: none"> • Faults in planning; • Unauthorized access; • Insufficient surveillance; • Insufficient air-conditioning; • Fire and smoke; • Water; • Power failure; and • Air ventilation and filtration. <p>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).</p>		
<p>The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.</p>	<p>Inspected Business Impact Analysis (BIA) Report for Google Data Centers, Data Center Access Policy, Third-Party Data Center Physical Security Requirements, Data Center Security Policy, Data Center Photo Policy, and Google EMEA Heating Ventilation and Air Conditioning (HVAC) Design Guidelines and Environmental Health and Safety (EHS) team Owner Project Requirements (OPR) to determine that the organization had policies and guidelines that governed how to keep the organization's physical workplaces, facilities, and property safe, which addressed risks stemming from the following:</p> <ul style="list-style-type: none"> - Faults in planning - Unauthorized access - Insufficient surveillance 	<p>No exceptions noted.</p>

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
	<ul style="list-style-type: none"> - 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 they 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.

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
<p>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).</p>		
<p>The organization's information processing resources are distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy, and availability.</p>	<p>Inspected the monitoring tool dashboard and the filesystem, datastore, and network configurations used for products and networks to determine that the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.</p>	<p>No exceptions noted.</p>
	<p>Inspected Google's CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups within the organization's information processing resources.</p>	<p>No exceptions noted.</p>
	<p>Inspected the replication tool dashboard and configurations to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy and availability.</p>	<p>No exceptions noted.</p>
	<p>Inspected system restoration testing results for a sample of products restored during the period to determine that backup restoration testing was completed and tracked via an audit log to support service redundancy and availability.</p>	<p>No exceptions noted.</p>

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
The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include 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 that covered reliability, survivability, and recovery at least annually.	No exceptions noted.
	Inspected the BIA documentation to determine that the potential impact to business operations was considered through a BIA.	No exceptions noted.
The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	Inspected the BIA documentation, the BC planning documentation, and the organization's ISO 27001 Statement of Applicability 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 and the assigned roles, responsibilities, risks, and recovery objectives within the BC Plan to determine that the organization had implemented business continuity measures to maintain the availability of the organization's production infrastructure and services.	No exceptions noted.
	Inspected documented recovery activities within 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.

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
<p>PS-03: Perimeter Protection</p> <p>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.</p> <p>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.</p>		
Data center perimeters are defined and secured via physical barriers.	Observed structural features such as a fenced perimeter, doors, walls, and segregated security zones for a sample of data centers to determine that data center perimeters were defined via physical barriers.	No exceptions noted.
	Observed locks on doors, security personnel monitoring facility and sensitive data center zones, and alerts generated by security systems to determine that data center perimeters were secured via physical security control mechanisms.	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 at a sample of data centers to determine that sensitive data centers zones were continuously monitored through the use of real-time video surveillance.	No exceptions noted.
	Observed security personnel monitoring facility buildings and campus through the use of 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.

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 "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 through the use of 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.
<p>PS-04: Physical Site Access Control</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
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 Cloud CISO Compliance & Certifications (C4) Team documentation to determine that two-factor authentication access control was required for sensitive data center zones and facility visitors were tracked and required to be escorted during their stay.	No exceptions noted.

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 at a sample of data centers to determine that two-factor authentication was enforced for access to sensitive data center zones through the use of badge readers, secondary identification mechanisms, and/or physical locks.	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 data center site access request tickets with business-need specific approvals and observed the visitor check-in process to determine that visitors were required to gain approval from authorized personnel.	No exceptions noted.
	Observed the visitor check-in process and the enforcement of escort requirements in facility spaces for a sample of data centers to determine that visitor identities were verified at facility perimeters and visitors were required to remain with escorts throughout the duration of their visits.	No exceptions noted.
Data center physical access logs are recorded and retained in accordance with organizational or regulatory requirements.	Inspected the configuration of the retention period 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 Security Logging Policy.	No exceptions noted.
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 in high-security areas in data centers were reviewed quarterly and inappropriate access was removed in a timely manner.	No exceptions noted.

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 Data Center Physical Access Policy to determine that automatic revocation of access would occur if a user had not accessed a data center for 2 months and that automatic withdrawal of access would occur if a user had not accessed a data center for 6 months.	Exception noted. The organization did not enforce the automatic revocation and automatic removal of data center access after 2 and 6 months of inactivity, respectively.
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 they 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.
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.

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
<p>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:</p> <p>a) Structural Measures:</p> <ul style="list-style-type: none"> • Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts. <p>b) Technical Measures:</p> <ul style="list-style-type: none"> • 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. <p>c) Organizational Measures</p> <ul style="list-style-type: none"> • Regular fire protection inspections to check compliance with fire protection requirements; and • Regular fire protection exercises. 		
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 data centers were equipped with fire detection alarms and protection equipment.	No exceptions noted.
	Inquired of facility personnel and observed the facility manager's presentation detailing fire drill procedures 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 data center structural parts were rated to maintain structural integrity for 90 minutes.	No exceptions noted.

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, such as generators, UPS systems, chillers, fire suppression systems in sensitive areas, emergency lighting, and HVAC systems, were continuously monitored and maintained through routine, regular inspections, 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.
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.

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
<p>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:</p> <p>a) Operational redundancy (N+1) in power and cooling supply</p> <p>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).</p> <p>c) Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>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).</p>	<p>Observed generators in person at a sample of data centers to determine that data centers were equipped with redundant power systems to support the continued operation of critical data center equipment in the event of the loss of the primary power source.</p>	<p>No exceptions noted.</p>
<p>Power management and distribution systems are utilized to protect critical data center equipment from disruption or damage.</p>	<p>Inspected the organization's data center security requirements for self-sufficient operation and the calculated generator fuel burn rates for a sample of data centers to determine that power management and distribution systems were utilized to protect critical data center equipment from disruption or damage and that data centers were capable of operating self-sufficiently for a minimum of 24 hours in the event of an external power failure per the organization's security requirements.</p>	<p>No exceptions noted.</p>

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 power and telecommunications equipment in data centers is physically protected from disruption and damage.	Observed facility managers' presentation detailing UPS capabilities, generator start-up times, and redundancy in cooling system design for a sample of data centers, to determine that data centers were appropriately equipped with redundant UPS systems and cooling systems to protect critical equipment from disruption and damage.	No exceptions noted.
	Inspected a sample of data centers to determine that the protection of power supply and telecommunications lines against interruption, interference, damage, and eavesdropping was checked at least every two years by qualified personnel.	No exceptions noted.
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, such as generators, UPS systems, chillers, fire suppression systems in sensitive areas, emergency lighting, and HVAC systems, were continuously monitored and maintained through routine, regular inspections, 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.
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.

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
<p>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.</p>		
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, such as generators, UPS systems, chillers, fire suppression systems in sensitive areas, emergency lighting, and HVAC systems, were continuously monitored and maintained through routine, regular inspections, 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.
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.

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
<p>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.</p>		
<p>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.</p>	<p>Inspected the organization's resource management documentation to determine that procedures related to the management of information processing resources were made available by the organization and that the procedures included guidance on requesting, monitoring, and maintaining resources and around forecasting future capacity requirements to identify usage trends and manage system overload.</p>	<p>No exceptions noted.</p>
<p>The organization manages the capacity of its information processing resources through a combination of planning, monitoring, and adjusting based on usage and system performance.</p>	<p>Inspected the annual planning index and timeline to determine that the capacity of the organization's information processing resources was managed through a combination of planning, monitoring, and adjusting based on usage and system performance.</p>	<p>No exceptions noted.</p>
	<p>Inspected the internal capacity monitoring dashboards to determine that the organization managed the capacity of its information processing resources through a combination of planning, monitoring, and adjusting based on usage and system performance.</p>	<p>No exceptions noted.</p>

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 required to be continuously monitored for events related to security, availability, processing integrity, and confidentiality threats and that alerts were required to be 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, processing integrity, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring tool dashboards, alert threshold configurations, and example alerts for events 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 within the customer portal to determine that the organization provided capacity and availability monitoring resources in a self-service portal for customers of cloud services to control and monitor the allocation of their system resources.	No exceptions noted.

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 capacity of the organization's information processing resources was managed through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
	Inspected the internal capacity monitoring dashboards to determine that the organization managed the capacity of its information processing resources through a combination of planning, monitoring, and adjusting based on usage and system performance.	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 ToS to determine that the organization's commitments to security, availability, processing integrity, 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, processing integrity, and confidentiality were communicated to external users via publications.	No exceptions noted.
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 the management of information processing resources were made available by the organization and that the procedures included guidance on requesting, monitoring, and maintaining resources and around forecasting future capacity requirements to identify usage trends and manage system overload.	No exceptions noted.

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
<p>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.</p>		
The organization provides monitoring capabilities for customers of cloud services.	Inspected monitoring dashboards within the customer portal to determine that the organization provided capacity and availability monitoring resources in a self-service portal for customers of cloud services to control and monitor the allocation of their system resources.	No exceptions noted.
<p>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:</p> <ul style="list-style-type: none"> • 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. 		
The organization has implemented mechanisms to protect its information assets against malicious activity (e.g. malware, spam, phishing).	Inspected the Vulnerability Management and System Security Policies and Guidelines to determine that mechanisms such as antivirus, antimalware, antispam, and antiphishing tools were required to be in place and that the instructions described the technical measures taken to securely configure, monitor, and protect both the customer and Google's cloud administration management console and information assets against malicious activity.	No exceptions noted.
	Inspected the global policy configuration of antivirus, antimalware, and antispam tools installed on each in-scope operating system type to determine that mechanisms were implemented to protect the organization's information assets against malicious activity.	No exceptions noted.

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
Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Inspected the documented administrative operations procedures for the organization's cloud computing environment on the external Quickstarts webpage to determine that administrative operations procedures were adequately 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 they 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.

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
<p>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.</p>		
<p>The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.</p>	<p>Inspected the Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and the Security Design in Applications, Systems, and Services Policy on the Company intranet to determine that the organization documented policies and procedures which required relevant personnel to use monitoring tools to facilitate the detection and reporting of operational issues.</p>	<p>No exceptions noted.</p>
	<p>Inspected monitoring tool dashboards, alerting configurations, and example alerts to determine that the organization provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.</p>	<p>No exceptions noted.</p>
<p>Integrity checks are in place at the file system level to ensure data integrity.</p>	<p>Inspected the file integrity monitoring dashboard and status reports of the integrity assurance system for an example node to determine that integrity checks were in place at the file system level, ensuring data integrity.</p>	<p>No exceptions noted.</p>
<p>Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.</p>	<p>Inspected monitoring tool configurations to determine that deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.</p>	<p>No exceptions noted.</p>

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 the Vulnerability Management and System Security Policies and Guidelines to determine that mechanisms such as antivirus, antimalware, antispam, and antiphishing tools were required to be in place and that the instructions described the technical measures taken to securely configure, monitor, and protect both the customer and Google's cloud administration management console and information assets against malicious activity.	No exceptions noted.
	Inspected the global policy configuration of antivirus, antimalware, and antispam tools installed on each in-scope operating system type to determine that mechanisms were implemented to protect the organization's information assets against malicious activity.	No exceptions noted.
<p>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.</p> <ul style="list-style-type: none"> • 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). 		
The organization maintains a framework that defines how to organize a response to security & privacy incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the organization maintained a framework that defined how to organize a response to security & privacy incidents.	No exceptions noted.

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 geographically dispersed personnel responsible for managing security incidents.	Inspected the security team internal webpage and the security team schedule to determine that the organization had geographically dispersed personnel responsible for managing security incidents.	No exceptions noted.
The organization's information processing resources are distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the monitoring tool dashboard and the filesystem, datastore, and network configurations used for products and networks to determine that the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups within the organization's information processing resources.	No exceptions noted.
	Inspected the replication tool dashboard and configurations to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected system restoration testing results for a sample of products restored during the period to determine that backup restoration testing was completed and tracked via an audit log to support service redundancy and availability.	No exceptions noted.

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 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 they 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.
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.		
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 the Security Design in Applications, Systems, and Services Policy on the Company intranet to determine that the organization documented policies and procedures which required relevant personnel to use monitoring tools to facilitate the detection and reporting of operational issues.	No exceptions noted.

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 example alerts to determine that the organization provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
The organization's information processing resources are distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the monitoring tool dashboard and the filesystem, datastore, and network configurations used for products and networks to determine that the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups within the organization's information processing resources.	No exceptions noted.
	Inspected the replication tool dashboard and configurations to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected system restoration testing results for a sample of products restored during the period to determine that backup restoration testing was completed and tracked via an audit log to support service redundancy and availability.	No exceptions noted.

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 maintains a framework that defines how to organize a response to security & privacy incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the organization maintained a framework that defined how to organize a response to security & privacy incidents.	No exceptions noted.
<p>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.</p>		
The organization's information processing resources are distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the monitoring tool dashboard and the filesystem, datastore, and network configurations used for products and networks to determine that the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups within the organization's information processing resources.	No exceptions noted.

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 replication tool dashboard and configurations to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected system restoration testing results for a sample of products restored during the period to determine that backup restoration testing was completed and tracked via an audit log to support service redundancy and availability.	No exceptions noted.
The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include 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 that covered reliability, survivability, and recovery at least annually.	No exceptions noted.
	Inspected the BIA documentation to determine that the potential impact to business operations was considered through a BIA.	No exceptions noted.

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.

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 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 be used to secure user data in transit between the organization's 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 the organization's production facilities.	No exceptions noted.
The organization's information processing resources are distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the monitoring tool dashboard and the filesystem, datastore, and network configurations used for products and networks to determine that the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups within the organization's information processing resources.	No exceptions noted.
	Inspected the replication tool dashboard and configurations to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected system restoration testing results for a sample of products restored during the period to determine that backup restoration testing was completed and tracked via an audit log to support service redundancy and availability.	No exceptions noted.

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
Data center perimeters are defined and secured via physical barriers.	Observed structural features such as a fenced perimeter, doors, walls, and segregated security zones for a sample of data centers to determine that data center perimeters were defined via physical barriers.	No exceptions noted.
	Observed locks on doors, security personnel monitoring facility and sensitive data center zones, and alerts generated by security systems to determine that data center perimeters were secured via physical security control mechanisms.	No exceptions noted.
<p>OPS-10: Logging and Monitoring – Concept</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
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 the organization had established guidelines that governed the installation of software on organization-owned assets.	No exceptions noted.
Security event logs are protected, and access is restricted to authorized personnel.	Inspected the Security Logging Policy and security event log protection configuration file to determine that security event logs were protected, and that access was restricted to authorized personnel.	No exceptions noted.

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 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 the Security Design in Applications, Systems, and Services Policy on the Company intranet to determine that the organization documented policies and procedures which required relevant personnel to use monitoring tools to facilitate the detection and reporting of operational issues.	No exceptions noted.
	Inspected monitoring tool dashboards, alerting configurations, and example alerts to determine that the organization provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	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 they 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.

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 geographically dispersed personnel responsible for managing security incidents.	Inspected the security team internal webpage and the security team schedule to determine that the organization had geographically dispersed personnel responsible for managing security incidents.	No exceptions noted.
<p>OPS-11: Logging and Monitoring – Metadata Management Concept</p> <p>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:</p> <ul style="list-style-type: none"> • 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 		
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 of the organization's services were provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.	No exceptions noted.

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
	Observed the customer account interface for an example environment to determine that customers of the organization's services were provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.	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 the procedures within the Data Categorization Guidelines to determine that the organization had policies and procedures in place that governed the use and protection of identifiable data.	No exceptions noted.
	Inspected the anonymization requirements, strategies, and procedures within the Data Anonymization Policy to determine that the organization had policies and procedures in place that required the anonymization of identifiable or pseudonymous production data before it could be used within non-production environments.	No exceptions noted.
	Inspected tickets and review documentation for a sample of anonymization reviews to determine that the organization required the anonymization of identifiable or pseudonymous production data before it could be used within non-production environments.	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 the Security Design in Applications, Systems, and Services Policy on the Company intranet to determine that the organization documented policies and procedures which required relevant personnel to use monitoring tools to facilitate the detection and reporting of operational issues.	No exceptions noted.

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 example alerts to determine that the organization provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	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 technical and organizational safeguards for the secure handling of metadata within the Data Security Policy to determine that the organization had security policies that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.	No exceptions noted.
	Inspected guidance and security policies related to metadata handled by product teams to determine that the organization had implemented security processes that defined the rules for collecting, accessing, processing, handling, retaining, and deleting 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 they 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.

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.
<p>OPS-12: Logging and Monitoring – Access, Storage and Deletion</p> <p>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:</p> <ul style="list-style-type: none"> • 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, at a minimum, audit logs included user ID, event type, timestamp, success or failure indication, event origination, and affected data or resource identifier and that audit logs were retained for a minimum of one year.	No exceptions noted.
	Inspected the log data deletion requirements within the Log Data Usage Rules, log retention configurations, and example audit logs to determine that audit logs were retained for at least one year and that log data was required to be deleted once it was no longer required for the purpose of which it was collected.	No exceptions noted.

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 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 threats to information security.	No exceptions noted.
	Inspected the job titles and organizational structures for a sample of personnel with logical access to audit logs to determine that logical access to audit logs 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.
	Inspected the documented technical and organizational safeguards for the secure handling of metadata within the Data Security Policy to determine that the organization had security policies that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.	No exceptions noted.
	Inspected guidance and security policies related to metadata handled by product teams to determine that the organization had implemented security processes that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.	No exceptions noted.

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 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 information according to 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 and security event log protection configuration file to determine that security event logs were protected, and that 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 the procedures within the Data Categorization Guidelines to determine that the organization had policies and procedures in place that governed the use and protection of identifiable data.	No exceptions noted.
	Inspected the anonymization requirements, strategies, and procedures within the Data Anonymization Policy to determine that the organization had policies and procedures in place that required the anonymization of identifiable or pseudonymous production data before it could be used within non-production environments.	No exceptions noted.
	Inspected tickets and review documentation for a sample of anonymization reviews to determine that the organization required the anonymization of identifiable or pseudonymous production data before it could be used within non-production environments.	No exceptions noted.

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
<p>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.</p>		
<p>The organization has a dedicated team responsible for managing security & privacy incidents.</p>	<p>Inspected the security team internal webpage and the security team schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.</p>	<p>No exceptions noted.</p>
<p>Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen & improve security controls, prevent future incidents, and can be used as examples for information security training.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>Inspected the root cause analysis and remediation documentation for a sample of security event tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, prevent future incidents, and could be used as examples for information security training.</p>	<p>No exceptions noted.</p>
	<p>Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.</p>	<p>No exceptions noted.</p>

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 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 required to be continuously monitored for events related to security, availability, processing integrity, and confidentiality threats and that alerts were required to be 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, processing integrity, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring tool dashboards, alert threshold configurations, and example alerts for events 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 client assets and an example of the client asset inventory review performed to determine that the organization maintained an updated, completed, accurate, valid, and consistent client device inventory throughout the asset lifecycle.	No exceptions noted.

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
<p>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.</p> <p>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).</p>		
<p>Customer data that is uploaded or created is encrypted at rest.</p>	<p>Inspected the organization's cryptographic policy and default encryption at rest webpage to determine that customer data uploaded or created was required to be encrypted at rest according to storage level encryption requirements.</p>	<p>No exceptions noted.</p>
	<p>Inspected the data backup encryption configurations and encryption configurations for storage devices with customer data to determine that customer data that was uploaded and created was encrypted at rest.</p>	<p>No exceptions noted.</p>
	<p>Inspected the Customer-Managed Encryption Keys guidance website to determine that encryption keys could be controlled by the end user.</p>	<p>No exceptions noted.</p>
<p>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.</p>	<p>Inspected log management tool configurations and example logs to determine that, at a minimum, audit logs included user ID, event type, timestamp, success or failure indication, event origination, and affected data or resource identifier and that audit logs were retained for a minimum of one year.</p>	<p>No exceptions noted.</p>

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 log data deletion requirements within the Log Data Usage Rules, log retention configurations, and example audit logs to determine that audit logs were retained for at least one year and that log data was required to be deleted once it was no longer required for the purpose of which it was collected.	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 be used to secure user data in transit between the organization's 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 the organization's production facilities.	No exceptions noted.
Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	Inspected the organization's Cryptographic Guidelines regarding encryption mechanisms to determine that the organization required the use of encryption to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
	Inspected the CDPA website made available to external users regarding encryption mechanisms to determine that the organization communicated to external users on how user authentication and administrator sessions transmitted over the internet were encrypted.	No exceptions noted.
	Inspected server scan results and configurations around encryption mechanisms to determine that the organization used encryption mechanisms to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.

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
	Observed a user and an administrator's connection settings to the organization's external websites to determine that encryption was 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 and security event log protection configuration file to determine that security event logs were protected, and that access was restricted to authorized personnel.	No exceptions noted.
The organization provides monitoring capabilities for customers of cloud services.	Inspected monitoring dashboards within the customer portal to determine that the organization provided capacity and availability monitoring resources in a self-service portal for customers of cloud services to control and monitor the allocation of 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, configurations for audit logging systems, and example logs to determine that audit logs were retained for auditable events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support the auditability of log data in the event that potentially suspicious or malicious activities were detected.	No exceptions noted.
	Inspected audit logging and monitoring tools at both the tenant level and Google's internal levels, as well as example audit logs, to determine that the organization retained audit logs covering privileged user access activities and authorized and unauthorized access attempts to support security incident investigation.	No exceptions noted.

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 required to be continuously monitored for events related to security, availability, processing integrity, and confidentiality threats and that alerts were required to be 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, processing integrity, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring tool dashboards, alert threshold configurations, and example alerts for events 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 within the customer portal to determine that the organization provided capacity and availability monitoring resources in a self-service portal for customers of cloud services to control and monitor the allocation of their system resources.	No exceptions noted.
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 the configurations for TLS protocol and the enforcement of two-factor authentication in the form of user ID with password, security key, and/or certificate to determine that access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No exceptions noted.

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 semi-annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to internal support tools was restricted to authorized personnel through the use of 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 threats to information security.	No exceptions noted.
	Inspected the job titles and organizational structures for a sample of personnel with logical access to audit logs to determine that logical access to audit logs 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 before being deployed.	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 systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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 a version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.

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 annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to the version control system was required to be approved.	No exceptions noted.
Security event logs are protected, and access is restricted to authorized personnel.	Inspected the Security Logging Policy and security event log protection configuration file to determine that security event logs were protected, and that access was restricted to authorized personnel.	No exceptions noted.
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 internal webpage and the security team schedule to determine that the organization had established a dedicated security team engaging in security and privacy of customer data and managing security 24/7 worldwide.	No exceptions noted.
The organization maintains a framework that defines how to organize a response to security & privacy incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the organization maintained a framework that defined how to organize a response to security & 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 required to be continuously monitored for events related to security, availability, processing integrity, and confidentiality threats and that alerts were required to be generated for further investigation.	No exceptions noted.

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 log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, processing integrity, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring tool dashboards, alert threshold configurations, and example alerts for events to determine that alerts were generated for further investigation.	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.
Audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts.	Inspected log monitoring dashboards, configurations for audit logging systems, and example logs to determine that audit logs were retained for auditable events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support the auditability of log data in the event that potentially suspicious or malicious activities were detected.	No exceptions noted.
	Inspected audit logging and monitoring tools at both the tenant level and Google's internal levels, as well as example audit logs, to determine that the organization retained audit logs covering privileged user access activities and authorized and unauthorized access attempts to support security incident investigation.	No exceptions noted.

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.
<p>OPS-18: Managing Vulnerabilities, Malfunctions and Errors – Concept</p> <p>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:</p> <ul style="list-style-type: none"> • 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, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security	No exceptions noted.

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
	patches applied based on the severity of the vulnerabilities and their assigned CVSS score.	
	Inspected the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring 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, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.	No exceptions noted.
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability and remediation planning meetings to determine that security teams met monthly 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 they 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.

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.
<p>OPS-19: Managing Vulnerabilities, Malfunctions and Errors – Penetration Tests</p> <p>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.</p> <p>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.</p>		
Penetration tests are performed using a methodology / frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes.	Inspected the annual penetration test results to determine that penetration tests were performed at least annually, using a methodology or frequency that aligned with compliance requirements and customer commitments.	No exceptions noted.
	Inspected remediation plans for vulnerabilities identified during the annual penetration test to determine that a remediation plan was developed, and changes were implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	No exceptions noted.

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
<p>The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.</p>	<p>Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.</p>	<p>No exceptions noted.</p>
	<p>Inspected the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring compliance with established security protocols for timely detection of system vulnerabilities.</p>	<p>No exceptions noted.</p>
	<p>Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.</p>	<p>No exceptions noted.</p>
	<p>Inspected calendar invites and agenda topics for a sample of monthly vulnerability and remediation planning meetings to determine that security teams met monthly to discuss identified vulnerabilities and remediation plans.</p>	<p>No exceptions noted.</p>

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
<p>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.</p>		
<p>The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.</p>	<p>Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.</p>	<p>No exceptions noted.</p>
	<p>Inspected the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring compliance with established security protocols for timely detection of system vulnerabilities.</p>	<p>No exceptions noted.</p>
	<p>Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.</p>	<p>No exceptions noted.</p>

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 and remediation planning meetings to determine that security teams met monthly 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 internal webpage and the security team 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 & 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 tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, 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 to determine whether they could have resulted in a failure to meet 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.

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 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.
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	No exceptions noted.

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
	procedures to ensure a quick, effective, and orderly response to information security incidents that were categorized by severity.	
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 & 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 tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, 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 to determine whether they could have resulted in a failure to meet 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 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.

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
<p>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.</p>		
<p>The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.</p>	<p>Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.</p>	<p>No exceptions noted.</p>
	<p>Inspected the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring compliance with established security protocols for timely detection of system vulnerabilities.</p>	<p>No exceptions noted.</p>
	<p>Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.</p>	<p>No exceptions noted.</p>

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 and remediation planning meetings to determine that security teams met monthly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
<p>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.</p>		
A standard image is utilized for the installation and maintenance of each production server.	Inspected the Change Management Policy and the organization's Source Code Guidelines to determine that a standard image was required to be utilized for the installation and maintenance of each production server.	No exceptions noted.
	Inspected monitoring tool configurations to determine that tools were configured to monitor production machines, detect deviations from pre-defined operating system configurations, and correct such deviations.	No exceptions noted.
	Inspected the log of the tool used to monitor the replication of the standard production image to determine that the tool was running in accordance with the schedule defined in the configuration.	No exceptions noted.
	Inspected the source code version control system configuration for the automated job used to verify production state images against their standard gold images every 40 minutes, as well as the configuration of the job used to automatically fix any deviations from the golden image, to determine that a standard image was utilized for the installation and maintenance of each production server.	No exceptions noted.

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 hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the Network Device and Configuration Guidelines to determine that the Company hardened virtual environments where the organization had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected the configuration of the tool used to enforce a standard production image for the installation and maintenance of Company servers to determine that the organization hardened virtual environments where it had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected customer image restriction functionality within the cloud portal and the default hardening standards for virtual machines and containers to determine that customers were provided mechanisms for the restriction of the available selections of default hardened images for virtual machines and containers to be used within their 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 and segmentation requirements for customer environments, infrastructure management, console management, and high risk environments within the organization's network diagrams and Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.	No exceptions noted.

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 the configuration for access control and authentication requirements for production network access to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that 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 the implementation of 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.

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 the procedures within the Data Categorization Guidelines to determine that the organization had policies and procedures in place that governed the use and protection of identifiable data.	No exceptions noted.
	Inspected the anonymization requirements, strategies, and procedures within the Data Anonymization Policy to determine that the organization had policies and procedures in place that required the anonymization of identifiable or pseudonymous production data before it could be used within non-production environments.	No exceptions noted.
	Inspected tickets and review documentation for a sample of anonymization reviews to determine that the organization required the anonymization of identifiable or pseudonymous production data before it could be used within non-production environments.	No exceptions noted.

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
<p>IDM-01: Policy for User Accounts and Access Rights</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.</p>	<p>Inspected authentication configurations for remote access to the corporate network, production machines, network devices, and support tools to determine that access to the corporate network, production machines, network devices, and support tools required a unique ID, password, and/or machine certificate.</p>	<p>No exceptions noted.</p>
	<p>Inspected network timeout configurations forcing active certificates to expire after 20 hours of inactivity to determine that the organization's network sessions were automatically timed out after 20 hours of inactivity.</p>	<p>No exceptions noted.</p>
<p>The organization has policies and guidelines that govern access to information systems.</p>	<p>Inspected the organization's access control policies to determine that the organization had policies and guidelines that governed access to information systems.</p>	<p>No exceptions noted.</p>

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 they 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.		
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 customer access to storage was managed through the application and that unique user IDs were utilized to enforce access separation between customer accounts.	No exceptions noted.

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
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 the Google Account or the BYOID authentication system prior to access being granted to cloud services to determine that external system users were identified and authenticated via the Google Account or the bring your own identity (BYOID) authentication system before access was granted to cloud services.	No exceptions noted.
	Inspected the customer account creation process used by external system users to create their own password to determine that external system users were identified and authenticated via the Google Accounts or the BYOID authentication system before access was granted to 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 deactivation process and configurations to determine that the organization had mechanisms in place that prevented 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 Account Security Policy and the Identity and Access Management Policy to determine that the organization separated duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	No exceptions noted.
	Observed an attempt to access a privileged system outside the realm of the user's job responsibilities to determine that the attempt to violate the separation of duties failed and that the organization separated duties and implemented a principle of least privilege by limiting access to only authorized users.	No exceptions noted.

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
<p>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.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>Inspected the access control management tool history log, tool configuration, and example new hire and transferred employees to determine that modifications to access control lists were recorded and approved by administrators.</p>	<p>No exceptions noted.</p>
<p>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.</p>	<p>Inspected the CDPA to determine that customers of the organization's services were provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.</p>	<p>No exceptions noted.</p>
	<p>Observed the customer account interface for an example environment to determine that customers of the organization's services were provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.</p>	<p>No exceptions noted.</p>

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
<p>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.</p>		
The organization has an established policy specifying the use of emergency credentials.	Inspected the Emergency Access Credential Policy to determine that the organization had an established policy that specified requirements for the use of emergency credentials.	No exceptions noted.
	Inspected the configuration for emergency credential expiration and a sample of emergency credential checkout tickets to determine that emergency credentials required approval from authorized personnel prior to checkout and that credentials expired 90 days after they were checked out.	No exceptions noted.
Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Inspected the critical access groups' code configuration that assigned reviews to the authorized group administrators to determine that critical access groups were reviewed at least annually.	No exceptions noted.
	Inspected critical access group user membership reviews performed by group administrators for a sample of products 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.
	Inspected automatic account revocation configurations to determine that inappropriate access identified as a result of the semi-annual critical access group membership reviews was removed at least hourly.	No exceptions noted.

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
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 to the corporate network, production machines, network devices, and support tools required a unique ID, password, and/or machine certificate.	No exceptions noted.
	Inspected network timeout configurations forcing active certificates to expire after 20 hours of inactivity to determine that the organization's 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 had documented procedures for terminating users with 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 it was configured to automatically remove access in a timely manner upon submission of a termination request by Human Resources or a manager.	No exceptions noted.

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's access to production machines, support tools, network devices, and corporate assets to determine that access was automatically removed in a timely manner by the automated tool used to revoke access 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 the organization maintained formal user registration and de-registration procedures 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 example new hire and transferred employees to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.

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
<p>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.</p>		
<p>Logical access to network devices is restricted to authorized personnel and is periodically reviewed.</p>	<p>Inspected the critical access groups' code configuration that assigned reviews to the authorized group administrators to determine that logical access to network devices was restricted to authorized personnel and was periodically reviewed.</p>	<p>No exceptions noted.</p>
	<p>Inspected critical access group user membership reviews performed by group administrators for a sample of network device reviews to determine that critical access group memberships were reviewed periodically to ensure that access was restricted appropriately and that reviews were tracked to completion.</p>	<p>No exceptions noted.</p>
<p>Critical access groups are reviewed on a periodic basis and inappropriate access is removed.</p>	<p>Inspected the critical access groups' code configuration that assigned reviews to the authorized group administrators to determine that critical access groups were reviewed at least annually.</p>	<p>No exceptions noted.</p>
	<p>Inspected critical access group user membership reviews performed by group administrators for a sample of products 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.</p>	<p>No exceptions noted.</p>

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 as a result of the semi-annual critical access group membership reviews was removed at least hourly.	No exceptions noted.
<p>IDM-06: Privileged Access Rights</p> <p>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.</p> <p>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.</p>		
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 was required to enforce two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	No exceptions noted.
	Inspected the code that enforced the authentication of users prior to granting the user a certificate to determine 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 and that certificates were only generated after a user was authenticated to single sign-on using two-factor authentication.	No exceptions noted.

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
Only users with a valid user certificate, corresponding private key, and appropriate authorization (per host) can access production machines via SSH.	Inspected the code that enforced the authentication of users prior to granting an authorized private key to determine that only users with a valid user certificate, corresponding private key, and appropriate authorization (per host) could access production machines via Secure Shell (SSH).	No exceptions noted.
	Inspected the configuration enforcing authorized key authentication to determine that it restricted SSH access to production machines from unauthorized users without a valid digital certificate.	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 Account Security Policy and the Identity and Access Management Policy to determine that the organization separated duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	No exceptions noted.
	Observed an attempt to access a privileged system outside the realm of the user's job responsibilities to determine that the attempt to violate the separation of duties failed and that the organization separated duties and implemented a principle of least privilege by limiting access to only authorized users.	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, configurations for audit logging systems, and example logs to determine that audit logs were retained for auditable events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support the auditability of log data in the event that potentially suspicious or malicious activities were detected.	No exceptions noted.

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 audit logging and monitoring tools at both the tenant level and Google's internal levels, as well as example audit logs, to determine that the organization retained audit logs covering privileged user access activities and authorized 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 had an established policy that specified requirements for the use of emergency credentials.	No exceptions noted.
	Inspected the configuration for emergency credential expiration and a sample of emergency credential checkout tickets to determine that emergency credentials required approval from authorized personnel prior to checkout and that credentials expired 90 days after they were checked out.	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 threats to information security.	No exceptions noted.
	Inspected the job titles and organizational structures for a sample of personnel with logical access to audit logs to determine that logical access to audit logs 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' code configuration that assigned reviews to the authorized group administrators to determine that critical access groups were reviewed at least annually.	No exceptions noted.

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 critical access group user membership reviews performed by group administrators for a sample of products 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.
	Inspected automatic account revocation configurations to determine that inappropriate access identified as a result of 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 the configurations for TLS protocol and the enforcement of two-factor authentication in the form of user ID with password, security key, and/or certificate to determine that access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No exceptions noted.
	Inspected the semi-annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No exceptions noted.
Logical access to network devices is restricted to authorized personnel and is periodically reviewed.	Inspected the critical access groups' code configuration that assigned reviews to the authorized group administrators to determine that logical access to network devices was restricted to authorized personnel and was periodically reviewed.	No exceptions noted.

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 critical access group user membership reviews performed by group administrators for a sample of network device reviews to determine that critical access group memberships were reviewed periodically 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.		
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 the organization required user data to only be processed 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 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.

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 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.
<p>IDM-08: Confidentiality of Authentication Information</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>Deviations are evaluated by means of a risk analysis and mitigating measures derived from this are implemented.</p>		
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 the organization had established formal guidelines for passwords to govern the management and use of authentication mechanisms.	No exceptions noted.

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 SSH idle time configurations propagated to servers to determine that they were configured to enforce password requirements in accordance with established formal guidelines for authentication mechanisms.	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 established formal guidelines for the management of authentication mechanisms.	No exceptions noted.
	Inspected the authentication configurations to determine that passwords were transmitted and stored in an encrypted procedure in accordance with established formal guidelines for passwords to govern the management and use of authentication mechanisms.	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 organization had a password change system that enforced the password guidelines defined in relevant security policies.	No exceptions noted.
	Observed a user attempt to change their password when password requirements were not met to determine that an error message was shown, 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 webpage to determine that customer data uploaded or created was required to be encrypted at rest according to storage level encryption requirements.	No exceptions noted.

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 data backup encryption configurations and encryption configurations for storage devices with customer data to determine that customer data that was uploaded and created was encrypted at rest.	No exceptions noted.
	Inspected the Customer-Managed Encryption Keys guidance website 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 was required to enforce two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	No exceptions noted.
	Inspected the code that enforced the authentication of users prior to granting the user a certificate to determine 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 and that certificates were only generated after a user was authenticated to single sign-on using two-factor authentication.	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 Account Security Policy and the Identity and Access Management Policy to determine that the organization separated duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	No exceptions noted.

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 realm of the user's job responsibilities to determine that the attempt to violate the separation of duties failed and that the organization separated duties and implemented a principle of least privilege by limiting access to only authorized users.	No exceptions noted.
The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected extended workforce personnel responsibilities and expected behavior for the protection of information within the confidentiality agreement template to determine that the organization 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 that 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.

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
<p>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.</p> <p>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.</p>		
<p>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.</p>	<p>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 installed on the connecting device and that it was required to enforce two-factor authentication in the form of user ID, password, security key, and/or certificate.</p>	<p>No exceptions noted.</p>
	<p>Inspected authentication configurations for remote access to corporate machines to determine that remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, as well as two-factor authentication in the form of user ID, password, security key, and/or certificate.</p>	<p>No exceptions noted.</p>
<p>Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.</p>	<p>Inspected the authentication configuration enforcing the required use of user IDs, passwords, security keys, and/or valid certificates for network device access to determine that logical access to organization-owned network devices was authenticated via user ID, password, security key, and/or certificate.</p>	<p>No exceptions noted.</p>

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
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 was required to enforce two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	No exceptions noted.
	Inspected the code that enforced the authentication of users prior to granting the user a certificate to determine 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 and that certificates were only generated after a user was authenticated to single sign-on using two-factor authentication.	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 the organization had established formal guidelines for passwords to govern the management and use of authentication mechanisms.	No exceptions noted.
	Inspected the SSH idle time configurations propagated to servers to determine that they were configured to enforce password requirements in accordance with established formal guidelines for authentication mechanisms.	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 established formal guidelines for the management of authentication mechanisms.	No exceptions noted.
	Inspected the authentication configurations to determine that passwords were transmitted and stored in an encrypted procedure in accordance with established formal guidelines for passwords to govern the management and use of authentication mechanisms.	No exceptions noted.

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
<p>Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.</p>	<p>Inspected the organization's security and privacy policies on the intranet to determine that they 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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>

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
<p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>The organization maintains policies that define the requirements for the use of cryptography.</p>	<p>Inspected the organization's Cryptographic Policy and the Account Authentication Security Guidelines to determine that the organization-maintained policies that defined the requirements for the use of cryptography.</p>	<p>No exceptions noted.</p>
<p>The organization prohibits the use of removable media for the storage of PII and SPII unless the data has been encrypted.</p>	<p>Inspected the Data Security Policy, Removable Media documentation, and the organization's Cryptographic Guidelines to determine that the organization prohibited the use of removable media for the storage of Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) unless the data had been encrypted.</p>	<p>No exceptions noted.</p>
<p>The organization has an established key management process in place to support the organization's use of cryptographic techniques.</p>	<p>Inspected the documented key management process within the organization's Cryptographic Guidelines to determine that the organization had an established key management process in place to support the organization's use of cryptographic techniques.</p>	<p>No exceptions noted.</p>

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 code configuration enforcing encryption and certificate authentication and revocation to determine that the organization had an established key management process in place to support the organization's use of cryptographic techniques.	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 they 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 Cryptographic Policy to determine that the organization had established guidelines for protecting against the risks of teleworking activities and that required the use of encrypted communication systems to access the system remotely.	No exceptions noted.

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 configuration that required the use of encryption to remotely authenticate to the system to determine that users could only access the system remotely through the use of 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 Guidelines to determine that the organization required the use of encryption protocols to secure user data in transit between users and the organization's production facilities.	No exceptions noted.
	Inspected the configuration that enforced encryption for all data in transit to determine that the organization enforced the required encryption protocols to secure user data in transit between users and the organization's production facilities.	No exceptions noted.
	Inspected test server reports, website certificates, and encryption protocol for the Google Cloud Platform (GCP) customer interface to determine that the organization encrypted end-user traffic while 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 Guidelines regarding encryption mechanisms to determine that the organization required the use of encryption to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
	Inspected the CDPA website made available to external users regarding encryption mechanisms to determine that the organization communicated to external users on how user authentication and administrator sessions transmitted over the internet were encrypted.	No exceptions noted.

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 server scan results and configurations around encryption mechanisms to determine that the organization used encryption mechanisms to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
	Observed a user and an administrator's connection settings to the organization's external websites to determine that encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No exceptions noted.
<p>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.</p>		
The organization maintains policies that define the requirements for the use of cryptography.	Inspected the organization's Cryptographic Policy and the Account Authentication Security Guidelines to determine that the organization-maintained policies that defined the requirements for the use of cryptography.	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 webpage 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 the data backup encryption configurations and encryption configurations for storage devices with customer data to determine that customer data that was uploaded and created was encrypted at rest.	No exceptions noted.

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 Customer-Managed Encryption Keys guidance website 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 documented key management process within the organization's Cryptographic Guidelines to determine that the organization had an established key management process in place to support the organization's use of cryptographic techniques.	No exceptions noted.
	Inspected the code configuration enforcing encryption and certificate authentication and revocation to determine that the organization had an established key management process in place to support the organization's use of cryptographic techniques.	No exceptions noted.

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.

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
<p>The organization has an established key management process in place to support the organization's use of cryptographic techniques.</p>	<p>Inspected the documented key management process within the organization's Cryptographic Guidelines to determine that the organization had an established key management process in place to support the organization's use of cryptographic techniques.</p>	<p>No exceptions noted.</p>
	<p>Inspected the code configuration enforcing encryption and certificate authentication and revocation to determine that the organization had an established key management process in place to support the organization's use of cryptographic techniques.</p>	<p>No exceptions noted.</p>

support@calfire.com

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
<p>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.</p>		
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 to determine that the organization documented the required use of monitoring tools to send automated alerts to operational personnel based on predetermined criteria and that incidents were required to be escalated per policy.	No exceptions noted.
	Inspected alert configurations and example alerts sent to operational personnel from monitoring tools to determine that monitoring tools were used to send automated alerts to operational personnel based on predetermined criteria and that incidents were escalated per policy.	No exceptions noted.
The organization has implemented mechanisms to protect the production environment from denial-of-service attacks.	Inspected the DoS protection documentation and incident management escalation playbooks to determine that mechanisms were in place to protect the production environment against a variety of DoS attacks.	No exceptions noted.
	Inspected the DoS thresholds, alerting configurations, and example DoS alerts within the monitoring dashboard to determine that effective mechanisms were in place to protect the production environment against a variety of DoS attacks.	No exceptions noted.

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 example alerts to determine that mechanisms were in place to detect and prevent 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 internal webpage and the security team schedule to determine that the organization had established dedicated teams who were responsible for monitoring, maintaining, managing, and securing 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 example configurations and alerts to determine that network traffic was monitored through a combination of automated and manual controls and processes to detect anomalous network events that could have indicated potential 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 required to be continuously monitored for events related to security, availability, processing integrity, and confidentiality threats and that alerts were required to be 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, processing integrity, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring tool dashboards, alert threshold configurations, and example alerts for events to determine that alerts were generated for further investigation.	No exceptions noted.

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 they 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.
<p>COS-02: Security Requirements for Connections in the Cloud Service Provider's Network</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
The organization's network security policies and guidelines apply to both physical and virtual networks.	Inspected the Network and Computer Security Policy and the Network Device Guidelines to determine that the organization's network security policies and guidelines applied to both physical and virtual networks.	No exceptions noted.

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 maintains production network diagrams, and uses support tools to manage and visualize networks.	Inspected the Data Security Policy, support tools, and documented network diagrams to determine that the organization-maintained production network diagrams and used support tools 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 Device and Configuration Guidelines to determine that the Company hardened virtual environments where the organization had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected the configuration of the tool used to enforce a standard production image for the installation and maintenance of Company servers to determine that the organization hardened virtual environments where it had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected customer image restriction functionality within the cloud portal and the default hardening standards for virtual machines and containers to determine that customers were provided mechanisms for the restriction of the available selections of default hardened images for virtual machines and containers to be used within their 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 and segmentation requirements for customer environments, infrastructure management, console management, and high risk environments within the organization's network diagrams and Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.	No exceptions noted.

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 the configuration for access control and authentication requirements for production network access to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.	No exceptions noted.
<p>COS-03: Monitoring of Connections in the Cloud Service Provider's Network</p> <p>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.</p> <p>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.</p>		
The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected the policies, design documentation, network topology diagrams, and firewall and global router configurations related to the perimeter devices to determine that the organization had implemented perimeter devices to protect the corporate network from external network 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 to determine that the organization documented the required use of monitoring tools to send automated alerts to operational personnel based on predetermined criteria and that incidents were required to be escalated per policy.	No exceptions noted.

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 example alerts sent to operational personnel from monitoring tools to determine that monitoring tools were used to send automated alerts to operational personnel based on predetermined criteria and that incidents were 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, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.	No exceptions noted.
	Inspected the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring 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, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.	No exceptions noted.

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 and remediation planning meetings to determine that security teams met monthly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
The organization conducts Information Security Risk Assessments at least annually 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 to identify and evaluate risks.	No exceptions noted.
	Inspected the risk assessment and the Internal Access Control program documents 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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 	No exceptions noted.

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
	<ul style="list-style-type: none"> - 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 internal webpage and the security team schedule to determine that the organization had established dedicated teams who were responsible for monitoring, maintaining, managing, and securing 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 the Network Device Guidelines to determine that the organization's 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 the DoS protection documentation and incident management escalation playbooks to determine that mechanisms were in place to protect the production environment against a variety of DoS attacks.	No exceptions noted.
	Inspected the DoS thresholds, alerting configurations, and example DoS alerts within the monitoring dashboard to determine that effective mechanisms were in place to protect the production environment against a variety of DoS attacks.	No exceptions noted.
The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected the policies, design documentation, network topology diagrams, and firewall and global router configurations related to the perimeter devices to determine that the organization had implemented perimeter devices to protect the corporate network from external network attacks.	No exceptions noted.

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 example alerts to determine that mechanisms were in place to detect and prevent 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 Data Security Policy, support tools, and documented network diagrams to determine that the organization-maintained production network diagrams and used support tools 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 and segmentation requirements for customer environments, infrastructure management, console management, and high risk environments within the organization's network diagrams and Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.	No exceptions noted.

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 the configuration for access control and authentication requirements for production network access to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that 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 example alerts to determine that mechanisms were in place to detect and prevent 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 the implementation of 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.

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 the policies, design documentation, network topology diagrams, and firewall and global router configurations related to the perimeter devices to determine that the organization had implemented perimeter devices to protect the corporate network from external network 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 and segmentation requirements for customer environments, infrastructure management, console management, and high risk environments within the organization's network diagrams and Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.	No exceptions noted.
	Inspected example network connection pathways within the network device monitoring tool and the configuration for access control and authentication requirements for production network access to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.	No exceptions noted.
Penetration tests are performed using a methodology / frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes.	Inspected the annual penetration test results to determine that penetration tests were performed at least annually, using a methodology or frequency that aligned with compliance requirements and customer commitments.	No exceptions noted.

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 annual penetration test to determine that a remediation plan was developed, and changes were implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	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 example alerts to determine that mechanisms were in place to detect and prevent unauthorized devices from connecting to the organization's network.	No exceptions noted.
<p>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.</p>		
The organization maintains production network diagrams, and uses support tools to manage and visualize networks.	Inspected the Data Security Policy, support tools, and documented network diagrams to determine that the organization-maintained production network diagrams and used support tools 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 and segmentation requirements for customer environments, infrastructure management, console management, and high risk environments within the organization's network diagrams and Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.	No exceptions noted.

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 the configuration for access control and authentication requirements for production network access to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that 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 the Account Authentication Security Guidelines to determine that the organization-maintained policies that defined the requirements for the use of cryptography.	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.

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 the documented technical and organizational safeguards for the secure handling of metadata within the Data Security Policy to determine that the organization had security policies that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.	No exceptions noted.
	Inspected guidance and security policies related to metadata handled by product teams to determine that the organization had implemented security processes that defined the rules for collecting, accessing, processing, handling, retaining, and deleting 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 they 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.

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
<p>PI-01: Documentation and Safety of Input and Output Interfaces</p> <p>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.</p> <p>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.</p>		
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 webpage 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 the policies, design documentation, network topology diagrams, and firewall and global router configurations related to the perimeter devices to determine that the organization had implemented perimeter devices to protect the corporate network from external network attacks.	No exceptions noted.
The organization maintains production network diagrams, and uses support tools to manage and visualize networks.	Inspected the Data Security Policy, support tools, and documented network diagrams to determine that the organization-maintained production network diagrams and used support tools to manage and visualize networks.	No exceptions noted.

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
Mechanisms are in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	Inspected firewall and network configurations and example alerts to determine that mechanisms were in place to detect and prevent unauthorized devices from connecting to the organization's network.	No exceptions noted.
<p>PI-02: Contractual Agreements for the Provision of Data</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>		
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 publicly available website to determine that the organization-maintained policies regarding the return, transfer, and disposal of user data and made these policies 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 ToS to determine that the organization's commitments to security, availability, processing integrity, 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, processing integrity, and confidentiality were communicated to external users via publications.	No exceptions noted.

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
<p>The organization has established policies and guidelines to govern data classification, labeling and security.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>Inspected the documented technical and organizational safeguards for the secure handling of metadata within the Data Security Policy to determine that the organization had security policies that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.</p>	<p>No exceptions noted.</p>
	<p>Inspected guidance and security policies related to metadata handled by product teams to determine that the organization had implemented security processes that defined the rules for collecting, accessing, processing, handling, retaining, and deleting metadata.</p>	<p>No exceptions noted.</p>
<p>The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.</p>	<p>Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential information according to the data retention and deletion policy.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>

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 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 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.
	Inspected 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 within the Company.	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 publicly available website to determine that the organization-maintained policies regarding the return, transfer, and disposal of user data and made these policies 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 information according to 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.

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 and Source Code Guidelines to determine that the organization had developed policies, procedures, and guidelines governing the secure development lifecycle.	No exceptions noted.
--	--	----------------------

	Inspected Security Requirements for Outsourced Software Development Policy to determine that outsourced development was required to be controlled according to requirements set forth in policies relevant to system development and acquisition and that applications were required to be tested and analyzed for vulnerabilities prior to acceptance.	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 systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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 a version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
--	--	----------------------

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 annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to the version control system was required to be approved.	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 they 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 & 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 where Google was a processor, with requirements being enforced via the SDPA addendum to contractual agreements or other data processing terms.	No exceptions noted.

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
<p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>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.</p>	<p>Inspected the Cloud Data Processing Addendum (CDPA) template to determine that the organization required external parties (Service Providers) to meet security & privacy requirements for safeguarding user data and that requirements were enforced via the "Information Protection Addendum (IPA)" or the "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.</p>	<p>No exceptions noted.</p>
	<p>Inspected the Inbound Service Agreement (ISA) and the Subprocessor Data Processing Agreement (SDPA) for a sample of processors and sub-processors supporting the in-scope systems to determine that the organization had implemented an addendum to contract with processors and sub-processors.</p>	<p>No exceptions noted.</p>
	<p>Inspected the termination clause for service issues related to vendors within an example ISA and an example SPDA 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.</p>	<p>No exceptions noted.</p>
<p>The organization has policies and guidelines governing the secure development lifecycle.</p>	<p>Inspected the Security Design in Applications, Systems, and Services Policy and Source Code Guidelines to determine that the organization had developed policies, procedures, and guidelines governing the secure development lifecycle.</p>	<p>No exceptions noted.</p>

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 Security Requirements for Outsourced Software Development Policy to determine that outsourced development was required to be controlled according to requirements set forth in policies relevant to system development and acquisition and that applications were required to be tested and analyzed for vulnerabilities prior to acceptance.	No exceptions noted.
The organization requires subprocessors to meet security & 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 where Google was a processor, with requirements being enforced via the SDPA addendum to contractual agreements or other data processing terms.	No exceptions noted.
<p>DEV-03: Policies for Changes to Information Systems</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		

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 change management requirements and procedures within the Change Management Security Policy and documented source code guidelines to determine that the organization had change management policies, procedures, and guidelines in place for tracking, testing, approving, and validating changes and that they included security code reviews.	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 to customer-facing services that could have affected security, confidentiality, processing integrity, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker webpage, 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, processing integrity, and availability.	No exceptions noted.

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 they 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.

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
<p>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.</p>		
<p>The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.</p>	<p>Inspected the internal Privacy Policy, Basic Security Policy, privacy and information security training program materials, and compliance monitoring tools to determine that a privacy and information security training program was established and that relevant personnel were required to complete this training annually.</p>	<p>No exceptions noted.</p>
	<p>Inspected the compliance monitoring tool dashboard used by management to monitor the completion rate for employees' completion of the required privacy and information security training, as well as configurations for the automated training enrollment tool, and an example of an email notification sent to employees for overdue training to determine that the organization had established a privacy and information security training program and that relevant personnel met the requirement to complete the training annually.</p>	<p>No exceptions noted.</p>
	<p>Inspected the security awareness training content to determine that security awareness training content was reviewed and updated at least annually.</p>	<p>No exceptions noted.</p>

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 change management requirements and procedures within the Change Management Security Policy and documented source code guidelines to determine that the organization had change management policies, procedures, and guidelines in place for tracking, testing, approving, and validating changes and that they included security code reviews.	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.

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 to customer-facing services that could have affected security, confidentiality, processing integrity, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker webpage, 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, processing integrity, and availability.	No exceptions noted.
<p>DEV-06: Testing Changes</p> <p>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.</p>		
The organization tests, validates, and documents changes to its services prior to deployment to production.	Inspected tickets for a sample of changes to the organization's services to determine that the organization tested, validated, and documented changes to its services 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 before being deployed.	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.

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
<p>The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.</p>	<p>Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.</p>	<p>No exceptions noted.</p>
	<p>Inspected the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring compliance with established security protocols for timely detection of system vulnerabilities.</p>	<p>No exceptions noted.</p>
	<p>Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.</p>	<p>No exceptions noted.</p>
	<p>Inspected calendar invites and agenda topics for a sample of monthly vulnerability and remediation planning meetings to determine that security teams met monthly to discuss identified vulnerabilities and remediation plans.</p>	<p>No exceptions noted.</p>

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-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 systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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 a version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected the annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to the version control system was required to be approved.	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 change management requirements and procedures within the Change Management Security Policy and documented source code guidelines to determine that the organization had change management policies, procedures, and guidelines in place for tracking, testing, approving, and validating changes and that they included security code reviews.	No exceptions noted.

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-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 systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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 a version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected the annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to the version control system was required to be approved.	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 change management requirements and procedures within the Change Management Security Policy and documented source code guidelines to determine that the organization had change management policies, procedures, and guidelines in place for tracking, testing, approving, and validating changes and that they included security code reviews.	No exceptions noted.

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-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 the documented change request tickets for a sample of manual network configuration changes to determine that manual changes to network configurations were reviewed and approved prior to deployment.	No exceptions noted.
	Inspected the documented change ticket for an example change deployed by the automated tool, following a pre-configured and manually reviewed network configuration change, to determine that automated changes to network configurations were reviewed and approved prior to deployment.	No exceptions noted.
	Inspected tickets for a sample of changes made to the automated deployment tool to determine that automated changes to network configurations 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 before being deployed.	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.

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 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 systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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 a version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected the annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to the version control system was required to be approved.	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.

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 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 the procedures within the Data Categorization Guidelines to determine that the organization had policies and procedures in place that governed the use and protection of identifiable data.	No exceptions noted.
	Inspected the anonymization requirements, strategies, and procedures within the Data Anonymization Policy to determine that the organization had policies and procedures in place that required the anonymization of identifiable or pseudonymous production data before it could be used within non-production environments.	No exceptions noted.
	Inspected tickets and review documentation for a sample of anonymization reviews to determine that the organization required the anonymization of identifiable or pseudonymous production data before it could be used within non-production environments.	No exceptions noted.

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
<p>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.</p>	<p>Inspected the physical and logical network architecture and segmentation requirements for customer environments, infrastructure management, console management, and high risk environments within the organization's network diagrams and Network Access Security Policies to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.</p>	<p>No exceptions noted.</p>
	<p>Inspected example network connection pathways within the network device monitoring tool and the configuration for access control and authentication requirements for production network access to determine that the organization segmented production, corporate, and non-production networks based on their nature and usage; that networks were physically and/or logically separated via access control mechanisms; that only approved use cases were allowed; and that exceptions required additional review and approval.</p>	<p>No exceptions noted.</p>

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
<p>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:</p> <ul style="list-style-type: none"> • 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 support tool dashboards to determine that the organization had developed policies and procedures that governed third-party relationships.	No exceptions noted.
	Inspected third-party information and associated agreement and relationship documentation within the vendor directory spreadsheet used for controlling and monitoring third parties to determine that the organization had developed processes that governed third-party relationships.	No exceptions noted.
Cloud Subprocessor security and privacy risk is assessed via periodic assessment of sub-processor control environment.	Inspected the VSA guide and VSA documentation for a sample of cloud sub-processors to determine that annual assessments of security and privacy risks of sub-processor control environments were performed.	No exceptions noted.

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 via business reviews during the period.	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.
	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 Cloud Data Processing Addendum (CDPA) template to determine that the organization required external parties (Service Providers) to meet security & privacy requirements for safeguarding user data and that requirements were enforced via the "Information Protection Addendum (IPA)" or the "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	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 the in-scope systems to determine that the organization had implemented an addendum to contract with processors and sub-processors.	No exceptions noted.

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 ISA and an example SPDA 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 they 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 & 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 where Google was a processor, with requirements being enforced via the SDPA addendum to contractual agreements or other data processing terms.	No exceptions noted.

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
<p>SSO-02: Risk Assessment of Service Providers and Suppliers</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>The organization conducts Information Security Risk Assessments at least annually to identify and evaluate risks.</p>	<p>Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment to identify and evaluate risks.</p>	<p>No exceptions noted.</p>
	<p>Inspected the risk assessment and the Internal Access Control program documents 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.</p>	<p>No exceptions noted.</p>
	<p>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:</p> <ul style="list-style-type: none"> - Administration of rights profiles, approval and assignment of access, and access authorizations - Development, testing, and release of changes - Operation of the system components 	<p>No exceptions noted.</p>

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
	<p>Inspected the risk assessment documentation to determine that the risk assessment evaluated the following risk areas:</p> <ul style="list-style-type: none"> - 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 sub-processor control environment.	Inspected the VSA guide and VSA documentation for a sample of cloud sub-processors to determine that annual assessments of security and privacy risks of sub-processor control environments were performed.	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 via business reviews during the period.	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.
	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.

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
<p>SSO-03: Directory of Service Providers and Suppliers</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>The information in the list is checked at least annually for completeness, accuracy and validity.</p>		
<p>Where the organization is a data processor, the organization maintains and makes available a list of subprocessors and updates that list, as contractually required.</p>	<p>Inspected the list of relevant sub-processors and the version history of the listing on the external Company website to determine that, where the organization was a data processor, the organization maintained and made available a list of sub-processors and updated that list as contractually required.</p>	<p>No exceptions noted.</p>

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
<p>SSO-04: Monitoring of Compliance with Requirements</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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).</p>		
<p>Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.</p>	<p>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.</p>	<p>No exceptions noted.</p>
<p>Cloud Subprocessor security and privacy risk is assessed via periodic assessment of sub-processor control environment.</p>	<p>Inspected the VSA guide and VSA documentation for a sample of cloud sub-processors to determine that annual assessments of security and privacy risks of sub-processor control environments were performed.</p>	<p>No exceptions noted.</p>
<p>Subprocessor performance is regularly assessed and monitored via periodic business reviews.</p>	<p>Inspected the Subprocessor Business Reports for a sample of subprocessors to determine that subprocessor performance was regularly assessed and monitored via business reviews during the period.</p>	<p>No exceptions noted.</p>
<p>The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.</p>	<p>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.</p>	<p>No exceptions noted.</p>

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 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 Vendor Security Assessment (VSA) Guidelines to determine that the Security Engineering Org had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
	Inspected the VSA review documentation, Quarterly Business Reports, and Monthly Business Reports for a sample of vendors to determine that the reviews included automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	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.

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
<p>SSO-05: Exit Strategy for the Receipt of Benefits</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		
<p>The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
<p>The organization conducts Information Security Risk Assessments at least annually to identify and evaluate risks.</p>	<p>Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment to identify and evaluate risks.</p>	<p>No exceptions noted.</p>
	<p>Inspected the risk assessment and the Internal Access Control program documents 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.</p>	<p>No exceptions noted.</p>

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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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 via business reviews during the period.	No exceptions noted.

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
<p>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.</p>		
<p>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).</p>	<p>Inspected the Security Incident Response Policy and security incident reporting sites on the Company intranet to determine that the organization provided internal personnel (employees and extended workforce) with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible teams.</p>	<p>No exceptions noted.</p>
<p>The organization has implemented a "follow the sun" model for its Security & Privacy Incident Response teams to ensure 24x7 coverage & continuity of operations.</p>	<p>Inspected the 24/7 on-call schedules for Security & Privacy Incident Response teams to determine that the organization had implemented a "follow the sun" model for its Security & Privacy Incident Response teams to ensure that operational responsibility hand-offs occurred routinely.</p>	<p>No exceptions noted.</p>
<p>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.</p>	<p>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 that were categorized by severity.</p>	<p>No exceptions noted.</p>

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 & 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 tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, 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 to determine whether they could have resulted in a failure to meet 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 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 & privacy incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the organization maintained a framework that defined how to organize a response to security & privacy incidents.	No exceptions noted.

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
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 they 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 internal webpage and the security team schedule to determine that the organization had established a dedicated security team engaging in security and privacy of customer data and managing security 24/7 worldwide.	No exceptions noted.
The organization has a dedicated team responsible for managing security & privacy incidents.	Inspected the security team internal webpage and the security team schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.	No exceptions noted.

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
<p>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.</p>		
<p>Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen & improve security controls, prevent future incidents, and can be used as examples for information security training.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>Inspected the root cause analysis and remediation documentation for a sample of security event tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, prevent future incidents, and could be used as examples for information security training.</p>	<p>No exceptions noted.</p>
	<p>Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.</p>	<p>No exceptions noted.</p>
	<p>Inspected security event 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.</p>	<p>No exceptions noted.</p>

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 & privacy incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the organization maintained a framework that defined how to organize a response to security & 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 that were categorized by severity.	No exceptions noted.
The organization has a dedicated team responsible for managing security & privacy incidents.	Inspected the security team internal webpage and the security team schedule to determine that the organization had a dedicated team responsible for managing security and privacy incidents.	No exceptions noted.
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 & 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.

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 the root cause analysis and remediation documentation for a sample of security event tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, 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 to determine whether they could have resulted in a failure to meet 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 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 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 that were categorized by severity.	No exceptions noted.

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 internal webpage and the security team 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 & privacy incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the organization maintained a framework that defined how to organize a response to security & 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.		
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 ToS to determine that the organization's commitments to security, availability, processing integrity, 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, processing integrity, and confidentiality were communicated to external users via publications.	No exceptions noted.

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 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.
	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 has established a code of conduct that is reviewed and updated as needed.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Information Security 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 are 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 & 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 tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, prevent future incidents, and could be used as examples for information security training.	No exceptions noted.

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 a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated to determine whether they could have resulted in a failure to meet 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 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 required to be continuously monitored for events related to security, availability, processing integrity, and confidentiality threats and that alerts were required to be 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, processing integrity, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
	Inspected monitoring tool dashboards, alert threshold configurations, and example alerts for events to determine that alerts were generated for further investigation.	No exceptions noted.

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, configurations for audit logging systems, and example logs to determine that audit logs were retained for auditable events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support the auditability of log data in the event that potentially suspicious or malicious activities were detected.	No exceptions noted.
	Inspected audit logging and monitoring tools at both the tenant level and Google's internal levels, as well as example audit logs, to determine that the organization retained audit logs covering privileged user access activities and authorized 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 to determine that the organization documented the required use of monitoring tools to send automated alerts to operational personnel based on predetermined criteria and that incidents were required to be escalated per policy.	No exceptions noted.
	Inspected alert configurations and example alerts sent to operational personnel from monitoring tools to determine that monitoring tools were used to send automated alerts to operational personnel based on predetermined criteria and that incidents were escalated per policy.	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 example alerts to determine that mechanisms were in place to detect and prevent unauthorized devices from connecting to the organization's network.	No exceptions noted.

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 internal webpage and the security team 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 & 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 tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen & improve security controls, 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 to determine whether they could have resulted in a failure to meet 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 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.

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
<p>BCM-01: Top Management Responsibility</p> <p>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.</p> <p>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.</p>		
The organization maintains a framework that defines how to organize a response to security & privacy incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the organization maintained a framework that defined how to organize a response to security & 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 documentation, the BC planning documentation, and the organization's ISO 27001 Statement of Applicability 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 and the assigned roles, responsibilities, risks, and recovery objectives within the BC Plan to determine that the organization had implemented business continuity measures to maintain the availability of the organization's production infrastructure and services.	No exceptions noted.
	Inspected documented recovery activities within 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.

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 the Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include 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 that covered reliability, survivability, and recovery at least annually.	No exceptions noted.
	Inspected the BIA documentation to determine that the potential impact to business operations was considered through a BIA.	No exceptions noted.
<p>BCM-02: Business Impact Analysis Policies and Instructions</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 		

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 the Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include 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 that covered reliability, survivability, and recovery at least annually.	No exceptions noted.
	Inspected the BIA documentation to determine that the potential impact to business operations was considered through a BIA.	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 Information Security Risk Assessments at least annually 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 to identify and evaluate risks.	No exceptions noted.

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 and the Internal Access Control program documents 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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.

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 they 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.

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);
- Methods for putting the plans into effect;
- Continuous process improvement; and
- Interfaces to Security Incident Management.

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 has geographically dispersed personnel responsible for managing security incidents.	Inspected the security team internal webpage and the security team schedule to determine that the organization had geographically dispersed personnel responsible for managing 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 documentation, the BC planning documentation, and the organization's ISO 27001 Statement of Applicability 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 and the assigned roles, responsibilities, risks, and recovery objectives within the BC Plan to determine that the organization had implemented business continuity measures to maintain the availability of the organization's production infrastructure and services.	No exceptions noted.
	Inspected documented recovery activities within 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.
The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.

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 DR and BC testing documentation and results for a sample of products to determine that the organization conducted disaster resiliency testing that covered reliability, survivability, and recovery at least annually.	No exceptions noted.
	Inspected the BIA documentation to determine that the potential impact to business operations was considered through a BIA.	No exceptions noted.
The organization's information processing resources are distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the monitoring tool dashboard and the filesystem, datastore, and network configurations used for products and networks to determine that the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected Google's CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups within the organization's information processing resources.	No exceptions noted.
	Inspected the replication tool dashboard and configurations to determine that the organization's information processing resources were distributed across at least two distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
	Inspected system restoration testing results for a sample of products restored during the period to determine that backup restoration testing was completed and tracked via an audit log to support service redundancy and availability.	No exceptions noted.

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 maintains a framework that defines how to organize a response to security & privacy incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the organization maintained a framework that defined how to organize a response to security & 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.		
The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include 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 that covered reliability, survivability, and recovery at least annually.	No exceptions noted.
	Inspected the BIA documentation to determine that the potential impact to business operations was considered through a BIA.	No exceptions noted.

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 ToS to determine that the organization's commitments to security, availability, processing integrity, 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, processing integrity, 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 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.
	Inspected 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 within the Company.	No exceptions noted.

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
<p>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:</p> <ul style="list-style-type: none"> • 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 the participating stakeholders involved in the coordination efforts for system security-related audits to determine that the organization planned and coordinated the 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 that required the independent audit of IT systems and components at least annually to determine that the organization had an internal audit function that was required to regularly engage with third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security and privacy and that the results, including findings and corrective actions of these reviews, were tracked and communicated to appropriate stakeholders via the ISMS documentation.	No exceptions noted.
	Inspected the organization's security compliance certifications obtained through independent audits of IT systems and components to determine that the organization regularly engaged third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security.	No exceptions noted.

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 they 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 had an established Internal Audit function that evaluated management's compliance with security controls annually.	No exceptions noted.

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, as well as tickets and documentation of the organization's risk assessment evaluations, to determine that the organization reviewed and validated the design, operation, and control record of in-scope compliance controls at least annually and that corrective actions were 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, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.	No exceptions noted.
	Inspected the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring 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, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.	No exceptions noted.

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 and remediation planning meetings to determine that security teams met monthly 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 that required the independent audit of IT systems and components at least annually to determine that the organization had an internal audit function that was required to regularly engage with third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security and privacy and that the results, including findings and corrective actions of these reviews, were tracked and communicated to appropriate stakeholders via the ISMS documentation.	No exceptions noted.
	Inspected the organization's security compliance certifications obtained through independent audits of IT systems and components to determine that the organization regularly engaged third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security.	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 they 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.

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 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.
<p>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.</p>		
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 the Security organizational charts on the Company's intranet to determine that information security was managed by an executive who was dedicated to Security, was independent of Information Technology responsibility, and had the ability to escalate security issues to the board level if necessary.	No exceptions noted.
	Inspected an example calendar invite and meeting agenda for a recent Security and Privacy team meeting to determine that a Security executive met with relevant personnel to discuss security issues and was able to escalate security concerns to the board level as necessary.	No exceptions noted.

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
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 board's documented oversight responsibilities relative to internal control within the Corporate Governance Guidelines and an example board meeting calendar invite and agenda topics to determine that all board of director members exercised independent judgment and that the independent / non-employee board of director members also demonstrated independence from management in exercising oversight of the development and performance of internal control.	No exceptions noted.
	Inspected a listing of the board of directors on the Investor Relations webpage 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 had an established Internal Audit function that evaluated management's compliance with security controls annually.	No exceptions noted.

support@calfire.ca.gov

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
<p>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.</p>		
<p>The organization establishes designated legal counsel and Government Affairs officials in order to maintain appropriate contacts with law enforcement authorities.</p>	<p>Inspected internal guidance and websites to determine that the organization established designated legal counsel and government affairs officials in order to maintain appropriate contacts with law enforcement authorities.</p>	<p>No exceptions noted.</p>
<p>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.</p>	<p>Inspected the Government Requests for Cloud Customer Data, the Google Cloud ToS, and internal process documentation to determine that the organization required mechanisms to be in place to ensure that customers were notified in accordance with any procedure and time periods agreed upon in the contract when legally required to disclose PII, unless such a disclosure was otherwise prohibited, and that the organization had procedures in place to produce data when required by applicable law, regulation, legal process, or enforceable governmental request.</p>	<p>No exceptions noted.</p>
	<p>Inspected the case management system, customer disclosure notes, and case details for example investigative request cases to determine that the organization had mechanisms in place to ensure that customers were notified in accordance with any procedure and time periods agreed upon in the contract when legally required to disclose PII, unless such a disclosure was otherwise prohibited, and that the organization produced data when required by applicable law, regulation, legal process, or enforceable governmental request.</p>	<p>No exceptions noted.</p>

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 the Government Requests for Cloud Customer Data, the Google Cloud ToS, and internal process documentation to determine that the organization required mechanisms to be in place to ensure that customers were notified in accordance with any procedure and time periods agreed upon in the contract when legally required to disclose PII, unless such a disclosure was otherwise prohibited, and that the organization had procedures in place to produce data when required by applicable law, regulation, legal process, or enforceable governmental request.	No exceptions noted.

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 case details for example investigative request cases to determine that the organization had mechanisms in place to ensure that customers were notified in accordance with any procedure and time periods agreed upon in the contract when legally required to disclose PII, unless such a disclosure was otherwise prohibited, and that the organization produced data when required by applicable law, regulation, legal process, or enforceable governmental request.	No exceptions noted.
<p>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.</p>		
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.

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
<p>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.</p>	<p>Inspected the Government Requests for Cloud Customer Data, the Google Cloud ToS, and internal process documentation to determine that the organization required mechanisms to be in place to ensure that customers were notified in accordance with any procedure and time periods agreed upon in the contract when legally required to disclose PII, unless such a disclosure was otherwise prohibited, and that the organization had procedures in place to produce data when required by applicable law, regulation, legal process, or enforceable governmental request.</p>	<p>No exceptions noted.</p>
	<p>Inspected the case management system, customer disclosure notes, and case details for example investigative request cases to determine that the organization had mechanisms in place to ensure that customers were notified in accordance with any procedure and time periods agreed upon in the contract when legally required to disclose PII, unless such a disclosure was otherwise prohibited, and that the organization produced data when required by applicable law, regulation, legal process, or enforceable governmental request.</p>	<p>No exceptions noted.</p>

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
<p>INQ-04: Limiting Access to or Disclosure of Data in Investigation Requests</p> <p>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.</p> <p>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.</p>		
<p>The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.</p>	<p>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.</p>	<p>No exceptions noted.</p>
	<p>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.</p>	<p>No exceptions noted.</p>
<p>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.</p>	<p>Inspected the Government Requests for Cloud Customer Data, the Google Cloud ToS, and internal process documentation to determine that the organization required mechanisms to be in place to ensure that customers were notified in accordance with any procedure and time periods agreed upon in the contract when legally required to disclose PII, unless such a disclosure was otherwise prohibited, and that the organization had procedures in place to produce data when required by applicable law, regulation, legal process, or enforceable governmental request.</p>	<p>No exceptions noted.</p>

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
	<p>Inspected the case management system, customer disclosure notes, and case details for example investigative request cases to determine that the organization had mechanisms in place to ensure that customers were notified in accordance with any procedure and time periods agreed upon in the contract when legally required to disclose PII, unless such a disclosure was otherwise prohibited, and that the organization produced data when required by applicable law, regulation, legal process, or enforceable governmental request.</p>	<p>No exceptions noted.</p>

support@comptia.com

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
<p>PSS-01: Guidelines and Recommendations for Cloud Customers</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.</p>		
<p>The organization provides information pertaining to the shared responsibilities of both itself and the cloud service customer.</p>	<p>Inspected the CDPA on the organization's website to determine that the organization provided information pertaining to the shared responsibilities of both itself and the cloud service customer.</p>	<p>No exceptions noted.</p>
<p>Customer responsibilities are described on the organization's product websites or in system documentation.</p>	<p>Inspected customer responsibilities on the organization's websites and in system documentation, as well as the Google Cloud Platform 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.</p>	<p>No exceptions noted.</p>

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 webpage 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 to customer-facing services that could have affected security, confidentiality, processing integrity, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker webpage, 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, processing integrity, and availability.	No exceptions noted.

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
<p>PSS-02: Identification of Vulnerabilities of the Cloud Service</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.</p>		
<p>The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.</p>	<p>Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.</p>	<p>No exceptions noted.</p>
	<p>Inspected the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring compliance with established security protocols for timely detection of system vulnerabilities.</p>	<p>No exceptions noted.</p>

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 tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.	No exceptions noted.
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability and remediation planning meetings to determine that security teams met monthly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
Penetration tests are performed using a methodology / frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes.	Inspected the annual penetration test results to determine that penetration tests were performed at least annually, using a methodology or frequency that aligned with compliance requirements and customer commitments.	No exceptions noted.
	Inspected remediation plans for vulnerabilities identified during the annual penetration test to determine that a remediation plan was developed, and changes were implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	No exceptions noted.
The organization has policies and guidelines governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy and Source Code Guidelines to determine that the organization had developed policies, procedures, and guidelines governing the secure development lifecycle.	No exceptions noted.

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 Security Requirements for Outsourced Software Development Policy to determine that outsourced development was required to be controlled according to requirements set forth in policies relevant to system development and acquisition and that applications were required to be tested and analyzed for vulnerabilities prior to acceptance.	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 before being deployed.	No exceptions noted.
<p>PSS-03: Online Register of Known Vulnerabilities</p> <p>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).</p> <p>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.</p>		
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.	No exceptions noted.

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 the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring 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, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.	No exceptions noted.
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability and remediation planning meetings to determine that security teams met monthly 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 to customer-facing services that could have affected security, confidentiality, processing integrity, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker webpage, 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, processing integrity, and availability.	No exceptions noted.

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 systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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 a version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected the annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to the version control system was required to be approved.	No exceptions noted.

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
- 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.

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
Security event logs are protected, and access is restricted to authorized personnel.	Inspected the Security Logging Policy and security event log protection configuration file to determine that security event logs were protected, and that 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, configurations for audit logging systems, and example logs to determine that audit logs were retained for auditable events such as privileged user access activities, authorized access attempts, and unauthorized access attempts to support the auditability of log data in the event that potentially suspicious or malicious activities were detected.	No exceptions noted.
	Inspected audit logging and monitoring tools at both the tenant level and Google's internal levels, as well as example audit logs, to determine that the organization retained audit logs covering privileged user access activities and authorized and unauthorized access attempts to support security incident investigation.	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.

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 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, at a minimum, audit logs included user ID, event type, timestamp, success or failure indication, event origination, and affected data or resource identifier and that audit logs were retained for a minimum of one year.	No exceptions noted.
	Inspected the log data deletion requirements within the Log Data Usage Rules, log retention configurations, and example audit logs to determine that audit logs were retained for at least one year and that log data was required to be deleted once it was no longer required for the purpose of which it was collected.	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 threats to information security.	No exceptions noted.
	Inspected the job titles and organizational structures for a sample of personnel with logical access to audit logs to determine that logical access to audit logs was restricted to authorized personnel.	No exceptions noted.

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
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 example configurations and alerts to determine that network traffic was monitored through a combination of automated and manual controls and processes to detect anomalous network events that could have indicated potential 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 the required use of user IDs, passwords, security keys, and/or valid certificates for network device access to determine that logical access to organization-owned network devices was authenticated via user ID, password, security key, and/or certificate.	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 the Google Account or the BYOID authentication system prior to access being granted to cloud services to determine that external system users were identified and authenticated via the Google Account or the bring your own identity (BYOID) authentication system before access was granted to cloud services.	No exceptions noted.

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 the customer account creation process used by external system users to create their own password to determine that external system users were identified and authenticated via the Google Accounts or the BYOID authentication system before access was granted to 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 was required to enforce two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	No exceptions noted.
	Inspected the code that enforced the authentication of users prior to granting the user a certificate to determine 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 and that certificates were only generated after a user was authenticated to single sign-on using two-factor authentication.	No exceptions noted.
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 the implementation of mechanisms by default to protect a customer's environment from other customers and unauthorized persons.	No exceptions noted.

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 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.
<p>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:</p> <ul style="list-style-type: none"> • 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. 		
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 organization had a password change system that enforced the password guidelines defined in relevant security policies.	No exceptions noted.
	Observed a user attempt to change their password when password requirements were not met to determine that an error message was shown, 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 the organization had established formal guidelines for passwords to govern the management and use of authentication mechanisms.	No exceptions noted.

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 the SSH idle time configurations propagated to servers to determine that they were configured to enforce password requirements in accordance with established formal guidelines for authentication mechanisms.	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 established formal guidelines for the management of authentication mechanisms.	No exceptions noted.
	Inspected the authentication configurations to determine that passwords were transmitted and stored in an encrypted procedure in accordance with established formal guidelines for passwords to govern the management and use of authentication mechanisms.	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 webpage 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 the data backup encryption configurations and encryption configurations for storage devices with customer data to determine that customer data that was uploaded and created was encrypted at rest.	No exceptions noted.
	Inspected the Customer-Managed Encryption Keys guidance website to determine that encryption keys could be controlled by the end user.	No exceptions noted.

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
<p>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").</p>		
Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Inspected the documented administrative operations procedures for the organization's cloud computing environment on the external Quickstarts webpage to determine that administrative operations procedures were adequately documented and made available to customers.	No exceptions noted.
<p>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).</p>		
The organization has an established policy specifying the use of emergency credentials.	Inspected the Emergency Access Credential Policy to determine that the organization had an established policy that specified requirements for the use of emergency credentials.	No exceptions noted.
	Inspected the configuration for emergency credential expiration and a sample of emergency credential checkout tickets to determine that emergency credentials required approval from authorized personnel prior to checkout and that credentials expired 90 days after they were checked out.	No exceptions noted.

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
<p>The organization separates duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.</p>	<p>Inspected the Account Security Policy and the Identity and Access Management Policy to determine that the organization separated duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.</p>	<p>No exceptions noted.</p>
	<p>Observed an attempt to access a privileged system outside the realm of the user's job responsibilities to determine that the attempt to violate the separation of duties failed and that the organization separated duties and implemented a principle of least privilege by limiting access to only authorized users.</p>	<p>No exceptions noted.</p>
<p>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.</p>	<p>Inspected the Account Authentication Guidelines to determine that personnel access to sensitive internal systems and applications was required to enforce two-factor authentication in the form of a distinct user ID and password with a security key or certificate.</p>	<p>No exceptions noted.</p>
	<p>Inspected the code that enforced the authentication of users prior to granting the user a certificate to determine 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 and that certificates were only generated after a user was authenticated to single sign-on using two-factor authentication.</p>	<p>No exceptions noted.</p>

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
<p>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.</p>		
<p>The organization has guidelines specifying the security requirements for new and existing information systems.</p>	<p>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.</p>	<p>No exceptions noted.</p>
<p>The organization tests, validates, and documents changes to its services prior to deployment to production.</p>	<p>Inspected tickets for a sample of changes to the organization's services to determine that the organization tested, validated, and documented changes to its services prior to deployment to production.</p>	<p>No exceptions noted.</p>
<p>Penetration tests are performed using a methodology / frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes.</p>	<p>Inspected the annual penetration test results to determine that penetration tests were performed at least annually, using a methodology or frequency that aligned with compliance requirements and customer commitments.</p>	<p>No exceptions noted.</p>
	<p>Inspected remediation plans for vulnerabilities identified during the annual penetration test to determine that a remediation plan was developed, and changes were implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.</p>	<p>No exceptions noted.</p>

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 webpage 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 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 the implementation of 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.
The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the organization had implemented a vulnerability management program, which included third-party penetration testing, to detect, remediate, and communicate system vulnerabilities, ensuring remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies, and tracked them within internal tools, with security patches applied based on the severity of the vulnerabilities and their assigned CVSS score.	No exceptions noted.

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 the vulnerability scanning frequency configurations, example monthly vulnerability scans, and scan results to determine that vulnerability scans were performed at least monthly, ensuring 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, initiated, and tracked within internal tools through to remediation for security deficiencies identified during vulnerability detection activities.	No exceptions noted.
	Inspected calendar invites and agenda topics for a sample of monthly vulnerability and remediation planning meetings to determine that security teams met monthly to discuss identified vulnerabilities and remediation plans.	No exceptions noted.
Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Inspected the documented administrative operations procedures for the organization's cloud computing environment on the external Quickstarts webpage to determine that administrative operations procedures were adequately 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 internal webpage and the security team schedule to determine that the organization had established dedicated teams who were responsible for monitoring, maintaining, managing, and securing the network.	No exceptions noted.

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's network security policies and guidelines apply to both physical and virtual networks.	Inspected the Network and Computer Security Policy and the Network Device Guidelines to determine that the organization's network security policies and guidelines applied to both physical and virtual networks.	No exceptions noted.
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: <ul style="list-style-type: none"> • 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 the organization communicated to cloud customers that customers were able to determine their data processing and storage locations where contractually available.	No exceptions noted.
	Inspected the cloud customer portal to determine that the organization allowed cloud customers to determine data processing and storage locations where contractually available.	No exceptions noted.
The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Inspected the Network Device and Configuration Guidelines to determine that the Company hardened virtual environments where the organization had a responsibility as outlined in the shared responsibilities.	No exceptions noted.

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 the configuration of the tool used to enforce a standard production image for the installation and maintenance of Company servers to determine that the organization hardened virtual environments where it had a responsibility as outlined in the shared responsibilities.	No exceptions noted.
	Inspected customer image restriction functionality within the cloud portal and the default hardening standards for virtual machines and containers to determine that customers were provided mechanisms for the restriction of the available selections of default hardened images for virtual machines and containers to be used within their cloud environment.	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 systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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 a version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
	Inspected the annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to the version control system was required to be approved.	No exceptions noted.

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 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 to customer-facing services that could have affected security, confidentiality, processing integrity, and availability.	No exceptions noted.
	Inspected official product blogs, public community support pages, the issue tracker webpage, 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, processing integrity, and availability.	No exceptions noted.
A standard image is utilized for the installation and maintenance of each production server.	Inspected the Change Management Policy and the organization's Source Code Guidelines to determine that a standard image was required to be utilized for the installation and maintenance of each production server.	No exceptions noted.
	Inspected monitoring tool configurations to determine that tools were configured to monitor production machines, detect deviations from pre-defined operating system configurations, and correct such deviations.	No exceptions noted.
	Inspected the log of the tool used to monitor the replication of the standard production image to determine that the tool was running in accordance with the schedule defined in the configuration.	No exceptions noted.
	Inspected the source code version control system configuration for the automated job used to verify production state images against their standard gold images every 40 minutes, as well as the configuration of the job used to automatically fix any deviations from the golden image, to determine that a standard image was utilized for the installation and maintenance of each production server.	No exceptions noted.

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
<p>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.</p>		
<p>The organization specifies and documents the countries and/or data center locations in which customer data might possibly be stored and transferred.</p>	<p>Inspected the available regions found on the Google Cloud locations site and the Google Cloud Platform console to determine that the organization specified and documented the countries and/or data center locations in which customer data might possibly be stored and transferred.</p>	<p>No exceptions noted.</p>
<p>The organization allows cloud customers to determine data processing and storage location in accordance with contractually defined options.</p>	<p>Inspected the CDPA to determine that the organization communicated to cloud customers that customers were able to determine their data processing and storage locations where contractually available.</p>	<p>No exceptions noted.</p>
	<p>Inspected the cloud customer portal to determine that the organization allowed cloud customers to determine data processing and storage locations where contractually available.</p>	<p>No exceptions noted.</p>

Section 5

Other Information Provided by Google LLC

support@corp.cloud

Management’s Response to Testing Exceptions

Assigned Controls	Results of Tests	Management’s Response
<p>Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.</p>	<p>Exception noted. The organization did not enforce the automatic revocation and automatic removal of data center access after 2 and 6 months of inactivity, respectively.</p>	<p>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.</p>

support@cora.cloud

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.