System and Organization Controls (SOC) 1 Type II Report

Description of the Google Cloud Platform System

For the Period 1 May 2023 to 30 April 2024

With Independent Service Auditor’s Assurance Report

Including Tests Performed and Results Thereof

Table of Contents

SECTION I - Google's Management Assertion

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Google’s Management Assertion

We have prepared the description of Google's Google Cloud Platform System entitled, "Description of the Google Cloud Platform System” (Description) for the Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) provided to user entities throughout the period 1 May 2023 to 30 April 2024 for user entities of the system during some or all of the period 1 May 2023 to 30 April 2024, and their auditors who audit and report on such user entities’ financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities’ financial statements.

Complementary user entity controls: The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Google’s controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

(a) The Description fairly presents the Google Cloud Platform System (System) made available to user entities of the System during some or all of the period 1 May 2023 to 30 April 2024 for the Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) provided to user entities as it relates to controls that are likely relevant to user entities’ internal control over financial reporting. The criteria we used in making this assertion were that the Description:

1. Presents how the System made available to user entities of the system was designed and implemented, including, if applicable:

    - The types of services provided
    - The procedures, within both automated and manual systems, by which those services are provided for user entities of the System
    - The information used in the performance of the procedures and supporting information; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities
    - How the System captures and addresses significant events and conditions
    - The process used to prepare reports and other information for user entities
    - Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them

- The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls
- Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided

2. Includes relevant details of changes to the System during the period covered by the Description
3. Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors, and may not, therefore, include every aspect of the Google Cloud Platform System that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment

(b) The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period 1 May 2023 to 30 April 2024 to achieve those control objectives, if user entities applied the complementary user entity controls assumed in the design of Google's controls throughout the period 1 May 2023 to 30 April 2024. The criteria we used in making this assertion were that:

1. The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization
2. The controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and
3. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority

Google LLC
08 July 2024

SECTION II - Independent Service Auditor's Assurance Report

Building a better
working world

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

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Independent Service Auditor's Assurance Report

To the Management of Google LLC:

Scope

We have examined Google LLC’s (referred to hereafter as “Google”) description entitled “Description of the Google Cloud Platform System” (Description) throughout the period 1 May 2023 to 30 April 2024 of its Google Cloud Platform system (System) for the Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) provided to user entities and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based on the criteria identified in "Google's Management Assertion" (Assertion). The Control Objectives and controls included in the Description are those that the management of Google believes are likely to be relevant to user entities’ internal control over financial reporting, and the Description does not include those aspects of the System that are not likely to be relevant to user entities’ internal control over financial reporting.

Complementary user entity controls: The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of Google’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Google’s responsibilities

Google has provided the accompanying assertion titled, "Google's Management Assertion", about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. Google is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Our examination was also performed in accordance with International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period 1 May 2023 to 30 April 2024. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives, based on the criteria in management's Assertion
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved
- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion

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

We apply International Standard on Quality Control I and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct all misstatements for the Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) provided to user entities. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying "Section IV - Description of Control Objectives, Controls, Tests and Results of Tests" (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the criteria described in Google's Assertion:

(a) The Description fairly presents the System that was designed and implemented throughout the period 1 May 2023 to 30 April 2024

(b) The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period 1 May 2023 to 30 April 2024 and user entities applied the complementary controls assumed in the design of Google's controls throughout the period 1 May 2023 to 30 April 2024

(c) The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period 1 May 2023 to 30 April 2024 if the user entity controls assumed in the design of Google's controls operated effectively throughout the period 1 May 2023 to 30 April 2024

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of Google, user entities of Google's System during some or all of the period 1 May 2023 to 30 April 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst + Young LLP

08 July 2024
San Jose, CA

SECTION III - Description of the Google Cloud Platform System

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Description of the Google Cloud Platform System

A. Overview of Operations

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

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

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

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

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

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

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

- Artificial Intelligence (AI) and Machine Learning (ML)
    - Agent Assist
    - AI Platform Deep Learning Container[2]
    - AI Platform Neural Architecture Search (NAS)
    - AI Platform Training and Prediction
    - Anti-Money Laundering (AML) AI
    - 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[1]

  - Document AI
  - Document AI Warehouse
  - Gemini for Google Cloud[1]
  - Generative AI on Vertex AI (formerly Generative AI Support on Vertex AI)
  - Recommendations AI[1]
  - Retail Search[1]
  - Speech-to-Text
  - Talent Solution
  - Text-to-Speech
  - Vertex AI Codey[2]
  - Vertex AI Colab Enterprise[2]
  - Vertex AI Conversation (formerly Generative AI App Builder)
  - Vertex AI Data Labeling
  - Vertex AI Platform (formerly Vertex AI)
  - Vertex AI Search (formerly Gen App Builder - Enterprise Search)[1]
  - Vertex AI Workbench Instances[2]
  - Video Intelligence API

- Application Programming Interface (API) Management

  - Advanced API Security[2]
  - Apigee
  - API Gateway
  - Application Integration[2]
  - Cloud Endpoints
  - Integration Connectors[2]

- Compute

  - App Engine
  - Batch
  - Compute Engine
  - Workload Manager[1]

- Data Analytics

  - BigQuery
  - Cloud Composer
  - Cloud Data Fusion
  - Cloud Life Sciences
  - Data Catalog
  - Dataflow
  - Dataform
  - Dataplex
  - Dataproc
  - Dataproc Metastore[1]
  - Looker Studio (formerly Google Data Studio)

  - Pub/Sub

- Databases

  - AlloyDB
  - Cloud Bigtable
  - Cloud Spanner
  - Cloud SQL
  - Datastore
  - Firestore
  - Memorystore

- Developer Tools

  - Artifact Analysis[2]
  - Artifact Registry
  - Cloud Build
  - Cloud Source Repositories
  - Cloud Workstations
  - Container Registry
  - Firebase Test Lab
  - Google Cloud Deploy
  - Google Cloud SDK
  - Infrastructure Manager[2]
  - Secure Source Manager[2]

- Healthcare and Life Sciences

  - Cloud Healthcare
  - Healthcare Data Engine (HDE)[1]

- Hybrid and Multi-cloud

  - Connect
  - Google Kubernetes Engine
  - GKE Enterprise Config Management (formerly Anthos Config Management)
  - GKE Identity Service (formerly Anthos Identity Service)
  - Hub
  - Knative serving (formerly Cloud Run for Anthos)
  - Service Mesh (formerly Anthos Service Mesh)

- Internet of Things (IoT)

  - IoT Core[6]

- Management Tools

  - Cloud Console
  - Cloud Console App

  - Cloud Deployment Manager
  - Cloud Shell
  - Recommenders
  - Service Infrastructure

- Media and Gaming

  - Game Servers[4]
  - Media CDN
  - Transcoder API

- Migration

  - BigQuery Data Transfer Service
  - Database Migration Service
  - Migration Center[1]
  - Migrate to Virtual Machines (formerly Migrate for Compute Engine)
  - Storage Transfer Service

- Networking

  - Cloud CDN
  - Cloud DNS
  - Cloud Firewall[1]
  - Cloud IDS (Cloud Intrusion Detection System)
  - Cloud Interconnect
  - Cloud Load Balancing
  - Cloud Network Address Translation (NAT)
  - Cloud Router
  - Cloud Service Mesh[2]
  - Cloud Virtual Private Network (VPN)
  - Google Cloud Armor
  - Network Connectivity Center
  - Network Intelligence Center
  - Network Service Tiers
  - Service Directory
  - Spectrum Access System
  - Traffic Director
  - Virtual Private Cloud (VPC)

- Operations
    - Cloud Debugger[5]
    - 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[2]
    - Cloud Asset Inventory
    - Cloud External Key Manager (Cloud EKM)
    - Cloud Hardware Security Module (HSM)
    - Cloud Key Management Service (KMS)
    - Firebase App Check
    - Firebase Authentication
    - Google Cloud Identity-Aware Proxy
    - Identity & 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[1]
  - Cloud Filestore
  - Cloud Storage
  - Cloud Storage for Firebase
  - Persistent Disk

- Other

  - Chronicle (SIEM)[3]
  - Google Cloud Threat Intelligence (GCTI) for Chronicle or Threat Intelligence for Chronicle[2]
  - Cloud Billing
  - Google Earth Engine
  - Google Cloud Marketplace
  - Tables

[1] Indicates products in scope only for the period 1 August 2023 through 30 April 2024

[2] Indicates products in scope only for the period 1 March 2024 through 30 April 2024

[3] Chronicle (SIEM) and Threat Intelligence for Chronicle are covered by separate terms than GCP. Refer to the Terms of Services (https://chronicle.security/legal/service-terms/) for additional details

[4] Game Servers was deprecated on June 30, 2023

[5] Cloud Debugger was deprecated on 16 May 2022 and the service was shut down on 31 May 2023

[6] IoT Core was deprecated on August 16, 2023

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

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

Artificial Intelligence (AI) and Machine Learning (ML)

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

Agent Assist

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

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)

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. 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 machine learning models with popular frameworks like TensorFlow, XGBoost and Scikit Learn. It provides scalable training and prediction services that work on large datasets.

Anti-Money Laundering (AML) AI

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

AutoML 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 machine learning models on structured data at increased speed and scale.

AutoML Translation

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

AutoML Video

AutoML Video delivers a simple and flexible machine learning 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 machine learning service that lets businesses and developers with limited machine learning 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 Application Programming Interface (API). Given a block of text, this API enables finding entities, analyzing sentiment (positive or negative), analyzing syntax (including parts of speech and dependency trees), and categorizing the content into a rich taxonomy. The API can be called by passing the content directly or by referring to a document in Cloud Storage.

Cloud Speaker ID

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

Cloud Translation

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

Cloud Vision

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

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

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 (formerly 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. Gemini for Google Cloud includes Gemini Code Assist.

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 large language, 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 machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.

Text-to-Speech

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

Vertex AI Codey

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

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

Vertex AI Colab Enterprise

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

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

Vertex AI Search (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. Users can interact with Vertex AI and other Google Cloud services from within a Vertex AI Workbench instance's Jupyter notebook.

Video Intelligence API

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

API Management

Advanced API Security

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

Apigee

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

API Gateway

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

Application Integration

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

Cloud Endpoints

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

Integration Connectors

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

Compute

App Engine

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

Batch

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

Compute Engine

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

Workload Manager

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

Data Analytics

BigQuery

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

Cloud Composer

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

Cloud Data Fusion

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

Cloud Life Sciences (formerly Google Genomics)

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

Data Catalog

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

Dataflow

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

Dataform

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

Dataplex

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

Dataproc

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

Dataproc Metastore

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

Looker 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, Cloud Pub/Sub allows communication between independent applications.

Databases

AlloyDB

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

Cloud Bigtable

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

Cloud Spanner

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

Cloud SQL

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

Datastore

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

Firestore

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

Memorystore

Memorystore for Redis (Remote Dictionary Server) provides a fully managed in-memory data store service for GCP. Cloud Memorystore can be used to build application caches that provide low latency data access. Cloud Memorystore is compatible with the Redis protocol, allowing seamless migration with no code changes.

Developer Tools

Artifact Analysis

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

Artifact Registry

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

Cloud Build

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

Cloud Source Repositories

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

Cloud Workstations

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

Container Registry

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

Firebase Test Lab

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

Google Cloud Deploy

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

Google Cloud SDK

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

Infrastructure Manager

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

Secure Source Manager

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

Healthcare and Life Sciences

Cloud Healthcare

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

Healthcare Data Engine (HDE)

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

Hybrid and Multi-cloud

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

Connect

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

Google Kubernetes Engine

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

GKE Enterprise Config Management (formerly Anthos 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 (formerly Anthos Identity Service)

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

Hub

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

Knative serving (formerly Cloud Run for Anthos)

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 (formerly Anthos 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)

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 Google Cloud Platform 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 the Google Cloud Platform. Cloud services can be procured, configured, and run from Cloud Console.

Cloud Console App

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

Cloud Deployment Manager

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

Cloud Shell

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

Recommender

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

Service Infrastructure

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

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

Media and Gaming

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. Stream media and deliver exceptional experiences to customer end users, no matter where they are.

Transcoder API

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

Migration

BigQuery Data Transfer Service

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

Database Migration Service

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

Migration Center

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

Migrate to Virtual Machines (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 down time by utilizing replication-based migration technology.

Storage Transfer Service

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

Networking

Cloud CDN

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

Cloud DNS

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

Cloud 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 Google Cloud Platform. This solution provides direct connection between on-premise networks and GCP Virtual Private Cloud.

Cloud Load Balancing

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

Cloud Network Address Translation (NAT)

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

Cloud Router

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

Cloud Service Mesh

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

Cloud Virtual Private Network (VPN)

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

Google Cloud Armor

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

Network Connectivity Center

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

Network Intelligence Center

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

Network Service Tiers

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

Service Directory

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

Spectrum Access System

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

Traffic Director

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

Virtual Private Cloud (VPC)

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

Operations

Cloud 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. It 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 Google Cloud Platform and other public cloud platforms. It includes monitor dashboards to display key metrics, define alerts and report on the health of cloud systems. The components of Cloud Logging that run on other public cloud platforms are not in scope for this report.

Cloud Monitoring

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

Cloud Profiler

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

Cloud Trace

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

Security and Identity

Access Approval

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

Access Context Manager

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

Access Transparency

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

Assured Workloads

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

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 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 (Cloud EKM)

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

Cloud Hardware Security Module (HSM)

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

Cloud Key Management Service (KMS)

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

Firebase App Check

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

Firebase Authentication

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

Google Cloud Identity-Aware Proxy

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

Identity & Access Management (IAM)

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

Identity Platform

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

Key Access Justifications (KAJ)

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

Managed Service for Microsoft Active Directory (AD)

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

reCAPTCHA Enterprise

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

Resource Manager API

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

Risk Manager

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

Secret Manager

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

Security Command Center

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

Sensitive Data Protection (including Cloud Data Loss Prevention 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 resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks.

Web Risk API

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

Serverless Computing

Cloud Functions

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

Cloud Functions for Firebase

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

Cloud Run

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

Cloud Scheduler

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

Cloud Tasks

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

Datastream

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

Eventarc

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

Workflows

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

Storage

Backup for GKE

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

Cloud Filestore

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

Cloud Storage

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

Cloud Storage for Firebase

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

Persistent Disk

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

Other

Chronicle (SIEM)

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

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

Google Cloud Threat Intelligence 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 either special review or logs that should be automatically sent to customers.

Cloud Billing

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

Google Earth Engine

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

Google Cloud Marketplace

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

Tables

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

Data Centers

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

North America, South America

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America

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

Europe, Middle East, and Africa

- Berlin (1), Germany

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

- Warsaw (3), Poland
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland*

Asia Pacific

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

+Indicates data center is in scope only for the period 1 August 2023 through 30 April 2024

*Indicates data center is in scope only for the period 1 November 2023 through 30 April 2024

**Indicates data center is in scope only for the period 1 March 2024 through 30 April 2024

B. Organization and Administration

Control Objective 1

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Internal Control Environment

Google has designed its internal control environment with the objective of providing reasonable assurance as to the integrity and availability of the data and user information, as well as the protection of assets from unauthorized use or disposition. Management has established and maintains an internal control structure that monitors compliance with established policies and procedures.

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform products or services to customers. The fundamentals underlying the services provided are the adoption of standardized, repeatable processes, the hiring and development of highly skilled resources, and leading industry practices.

Formal organizational structures exist and are available to Google personnel, including employees, temporary workers, vendors, and contractors on the Company's intranet. The intranet provides drill-down functionality for identifying personnel in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Security and privacy policies are reviewed annually, and other materials derived from policies, like guidelines, frequently asked questions (FAQs), and other related documents are reviewed and updated as needed. Databases and web sites exist to track and monitor the progress of Google Cloud Platform project developments. Google establishes agreements, including non-disclosure agreements, for preserving the confidentiality of information and software exchange with external parties.

To maintain internal compliance, Google has established a disciplinary process for non-compliance with the Code of Conduct, company policies, and other personnel requirements which could include dismissal, lawsuits and/or criminal prosecution. Moreover, Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product related controls over change management, access management, configuration management, security management, redundancy management, incident management, and capacity management.

The organization utilizes technologies to support the workforce in both remote and office work environments.

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 employees understand their roles and responsibilities and to help ensure that significant events are communicated in a timely manner. These methods include:

- Orientation and training programs for newly hired employees
- An information security training program that is required to be completed by relevant personnel annually
- Organization personnel are required to acknowledge the code of conduct
- Regular management meetings for updates on business performance and other business matters
- Company goals and responsibilities are developed and communicated by management on a periodic basis and amended as needed. Results are evaluated and communicated to employees
- Detailed job descriptions, product information (including system and its boundaries), and Google's security, availability, and confidentiality obligations that are made available to employees in the intranet
- The use of electronic mail messages to communicate time-sensitive messages and information
- Publishing security policies and security related updates in the intranet, which is accessible by all Google employees, temporary workers, contractors, and vendors

Google has also implemented various methods of communication to help ensure that user entities understand Google's commitments to security, availability, and confidentiality for Google Cloud Platform; and to help ensure that significant events are communicated to user entities in a timely manner. The primary conduit for communication is the Google website, which is made available to all user entities. This includes blog postings on the Official Google Blog, various product specific blogs, support forums and release notes. Google provides 24 x 7 assistance, including online and phone support to address customers' concerns. Customer service and/or technical support representatives are also an important communication channel, as they maintain records of problems reported by the user entity. Customer service representatives also assist in communicating information regarding new issues and/or developments, changes in services, and other information. Additionally, Google maintains an established Board of Directors that operates independently from management. The Board exercises oversight over management decisions.

Information Security Program

Google's Information Security program is designed to safeguard information assets against unauthorized use, disclosure, modification, damage, or loss. The program includes educating Google personnel about security related issues, assessing current policies and developing new policies, assisting in strengthening technical measures to protect corporate resources, and developing mechanisms to react to incidents and events that could affect Google's information assets.

Google has dedicated security teams responsible for educating Google personnel about security and assisting product teams with security design. Information security is managed by a dedicated Security and Privacy executive who is independent of Information Technology management responsibilities and may escalate security issues or concerns directly to the board. The Security Team also reviews the security practices of vendors and the security posture of vendor products for all vendors that Google shares confidential or sensitive information with.

Google has security policies that have been reviewed and approved by management and are published and communicated to employees and extended workforce (i.e. temporary workers, vendors, and contractors) with access to the Google intranet. Google's security policies describe security objectives, provide a security framework, and emphasize the importance of security to Google's business. Security policies are reviewed at least annually. Policies, FAQs, and guidelines are updated as needed.

Hiring Practices

Google has designed formal global hiring practices to help ensure that new, rehired, or transferred employees are qualified for their functional responsibility. Every employee has a written job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Google. Where local labor law or statutory regulations permit, Google may conduct criminal, credit, and/or security checks on all potential employees, temporary workers, and independent contractors, as well as verification of the individual's education, previous employment, and referrals. The specifics or extent of background checks performed depend on the position and location for which the individual is applying.

Upon acceptance of employment, all employees including extended workforce personnel are required to execute a confidentiality agreement as well as acknowledge receipt and compliance with Google's Code of Conduct. The confidentiality and privacy of customer data is emphasized in the handbook and also during new employee orientation. It is the responsibility of every employee to timely communicate significant issues and exceptions to an appropriate higher level of authority within the Company.

Risk Management

Risk management is a pervasive component of Google Cloud Platform's products, irrespective of the location or business area. The Google teams which lead engineering, sales, customer service, finance, and operations have the primary responsibility to understand and manage the risks associated with their activities for user entities using Google Cloud Platform's products. These risk management and mitigation activities have been integrated into Google's repeatable process model.

At a corporate level there are multiple functional areas including: Legal, Information Security, Internal Audit, Privacy Engineering, Compliance Assurance and Advisory, CSRM (Compliance, Security, and Risk Management), Ethics and Business Integrity, OCI (Office of Compliance and Integrity), ARRIS (Alphabet Regulatory Response Investigations & Strategy) and PSS (Privacy, Security and Safety), that provide risk management support through policy guidelines and internal consulting services.

Google develops and maintains a risk management framework to manage risk to an acceptable level for the Google Cloud Platform. Google has developed vulnerability management guidelines and regularly analyzes the vulnerabilities associated with the system environment. Google takes into consideration various threat sources such as insider attacks, external attacks, errors and omissions, and threats related to third parties such as the inadvertent disclosure of Google confidential information (for example, payroll data) by a third party.

Monitoring

Management performs periodic assessments of the control environment including areas such as identity management, source code management, physical security, and authentication infrastructure controls. Google's internal compliance team also performs regular internal audits and independent third-party audits over these areas of the control environment. The reports associated with these internal audits are reviewed in executive meetings and made available to the audit committee and stakeholders. In addition, monitoring activities have been described below to communicate how monitoring is performed for the Google Cloud Platform.

C. Logical Access

Control Objective 2

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Network Architecture and Management

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

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

Authentication, Authorization, and Administration

Authentication and access controls are implemented to restrict access to Google Cloud Platform production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) and Secure Sockets Layer (SSL) certificates, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google uses encryption to secure user data in transit between Google production facilities.

Access to internal support tools, those used by Google operational staff to maintain and troubleshoot the systems for Google Cloud Platform is controlled via access control lists (ACLs) thus limiting the use of these tools to only those individuals that have been authorized. Digital certificates used for machine authentication and data encryption are issued by an internal Google certificate authority. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet. Remote access to the Google corporate machines requires a Google-issued digital certificate installed on the connecting device and two-factor authentication.

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

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

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

Password Guidelines

Google personnel are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection and management guidelines, which enforce the following:

- Minimum length
- Complexity
- History
- Idle time lockout setting

Password configuration requirements are enforced by internal systems. In addition to the security requirements enforced during configuration, internal passwords are subject to cryptographic hashing to mitigate the risk of unauthorized disclosure or modification.

Google has supplemented passwords with a two-factor authentication requirement for internal personnel to access sensitive internal corporate and production services and to access Google Cloud Platform in the production environment from the corporate network. Two-factor authentication provides additional protection to prevent user account manipulation in case the user’s password is compromised.

Google Cloud Platform end-users can also authenticate in one of three ways:

- Using their user ID and a password that is managed by Google
- Using a two-step authentication process that includes their user ID, password, and a security key
- Through the Security Assertion Markup Language (SAML) based Single Sign-On (SSO) process which uses the user entity’s own account management system to authenticate users and a certificate with an embedded public key, which is registered with Google for each customer entity.

Security Monitoring

Google has implemented monitoring tools to detect and report security events. Antivirus, phishing detection, secure coding, and antimalware/antispam tools are in place to protect Google's information assets. Google also maintains and protects security event logs for privileged access, access to user data, authorized, and unauthorized access attempts. Security event logs are monitored continuously using a Google proprietary Security Information and Event Management (SIEM) system to detect intrusion attempts and other security related events. The SIEM is supplemented with codified logic which creates the “hunts” that trigger automated alerts to security personnel. The security alerts are triaged through manual or automated actions and further investigated based on predefined thresholds.

D. Change Management

Control Objective 3

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Overview

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

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

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

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

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

Guidelines are made available internally to govern the installation of software on organization-owned assets. Additionally, tools are utilized to automatically synchronize operating system (OS) configurations on production machines and correct them if deviations from the baseline image are detected. This enables a consistent deployment of updates to system files and helps ensure that machines remain in a known current-state. Mobile code is also blocked by default via standard web browser configurations on company owned endpoints.

Data Retention and Deletion

Google has procedures in place to dispose of confidential 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.

E. Physical Security

Control Objective 4

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Overview

Google maintains consistent policies and standards across its data centers for physical security to help protect production servers, network devices, and network connections within Google Data Centers. Guidelines for evaluating the security of data centers are described in Google's Data Center security evaluation criteria. Additionally, data center personnel perform periodic surveys and reviews of data centers. Data centers that house Google Cloud Platform systems and infrastructure components are reviewed and assessed periodically for ongoing security compliance. A security report is then created summarizing any observations, deviations, or action items. This report is presented to executive management for review and approval. Corrective actions are taken when necessary. The data center security evaluation criteria elements include:

- Existence of security guards, access badges, and video cameras
- Entrances, cages, suites, and rooms in use by Google are secured by either badge readers, secondary identification mechanisms, and/or physical locks
- Emergency exit points from server rooms are alarmed
- Video cameras exist to monitor the interior and exterior of the facility
- 24 x 7 on-site security personnel

Formal access procedures exist for allowing physical access to the data centers. There are documented procedures for issuing badges to staff and/or visitors and the owner of each badge is tracked and documented. All entrants to the data center, whether they are Google employees, visitors, or contractors, must identify themselves as well as show proof of identity to Security Operations.

Valid proof of identity consists of a photo ID issued by (1) Google or (2) a governmental entity. Only validated visitors and authorized Google employees and contractors are permitted to enter the data centers. Authorized Google Data Center Approvers must approve all visitors in advance for the specific data center and internal areas they wish to visit.

After the individual's access authorization is verified, the visit is logged, and access is granted for the specified dates and times. These logs are retained by Google security for review as needed. Visitors are provided a temporary badge and must be escorted by an authorized Google employee. When the visitors leave the data center, they must return the visitor badge.

Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas. Google authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items. Google also utilizes automated mechanisms to track inventory of all production machines and inventory of all serialized server components. Only authorized Google employees or contractors permanently working at the data centers are permitted to request standing access to the facility areas needed for their role and responsibilities. Data center access requests must be made through internal tools and require the approval of authorized data center personnel. All other Google employees and authorized contractors requiring temporary data center access must also have an approved access request and register at the guard station upon arrival. User access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.

Data centers are equipped with fire detection alarms and protection equipment. Data center server floors and network infrastructure are connected to redundant power sources that are physically protected from disruption and damage in addition to emergency power which is available in the event of a loss of power. Google performs preventative and regular maintenance on fire detection and protection equipment, Uninterruptible Power Supply (UPS), generators, HVAC, and emergency lighting systems. Refer to Section A for a list of Google's Data Center locations.

F. Incident Management

Control Objective 5

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Incident Management

Dedicated on-call personnel and incident response teams are responsible for managing, responding to, and tracking incidents. These teams are organized into formalized shifts and are responsible for helping resolve emergencies 24 x 7. Incident response policies are in place and procedures for handling incidents are documented.

Incident Alert and Recording

Automated signals generate alerts whenever an anomaly occurs. Production monitoring tools, in response to an anomaly, automatically generate alerts to relevant teams. An anomaly may also be manually documented by Google personnel when an issue is identified in response to a customer service request or reported through externally available channels.

Production systems are configured to send system events to monitoring and alerting tools. Google personnel use these tools to respond to potential incidents, including, but not limited to, security incidents.

Alerts capture information necessary for initial response (e.g., origin, service description, impacted area, etc.). Alerts are addressed by relevant teams to identify if the anomaly indicates an issue or potential issue. If necessary, incidents are created for alerts that require additional investigation. Additional details can be added to the incident to supplement the initial alert(s). The incident is assigned an initial severity level, which is used to prioritize mitigation efforts to incidents of greatest severity. Each severity level has been formally defined to capture the importance of each incident/problem type. There are established roles and responsibilities for personnel tasked with incident management, including the identification, assignment, managed remediation, and communication of incidents.

Incident Escalation

Google has documented escalation procedures and communication protocols that address the handling of incidents and notifying appropriate individuals. Escalated issues are treated with higher urgency and often shared with a wider audience.

Alert escalation is facilitated by an internal escalation tool or manual escalation based on Google-wide and team-specific escalation criteria. Production monitoring tools are integrated with the alert manager tool and communicated with the escalation tool. The escalation time and contacts are defined in the escalation tool configuration files. This leads to automated escalation if the tool does not receive an acknowledgement from the notified contacts.

Incident Resolution

After gathering the necessary information about the incident, the incident ticket is assigned to the appropriate support area based on the nature of the problem and/or the root cause. Incidents are usually forwarded to one of the corresponding technical departments:

- System Reliability Engineers / Software Engineers
- Networks
- Database Administration
- System Administration
- Application Administration
- Facilities
- Network Security
- Platform Support

The incident ticket is closed upon resolution of the incident. Google also has an established process for performing technical analysis of incidents after the fact to identify root cause issues, document lessons learned, and implement fixes to strengthen and improve security controls, and prevent future incidents.

G. Availability

Control Objective 6

Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.

Overview

Google Cloud Platform runs in a multi-tenant, distributed environment on synchronized internal system atomic clocks and global positioning systems (GPS). Rather than segregating user-entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For Google Cloud Platform, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Customer data is then stored in large, distributed databases, built on top of this file system. Where applicable, alternate storage procedures are documented and in place for backing up and recovering customer data. Backups are periodically performed to support the availability of customer data, and restore tests are periodically performed to confirm the ability to recover user data.

Redundant architecture exists such that data is replicated in real-time to at least two geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Management of the data centers is also distributed to provide location-independent, around the clock coverage and system administration. Google uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location. Additionally, business continuity plans defining how personnel should respond to disruptions are made available internally and maintained.

H. Complementary User Entity Control Considerations

Google Cloud Platform is designed with the assumption that user entities (also referred to as customers) would implement certain policies, procedures, and controls. In certain situations, the application of specific or additional controls at the user entity may be necessary to achieve the control objectives stated in the description. Therefore, each user's controls must be evaluated in conjunction with the controls summarized in Section III and Section IV of this report.

This section describes those additional policies, procedures, and controls that Google recommends user entities should consider to complement Google's policies, procedures, and controls. Management of the user entity and the user entity's auditor should consider whether the following controls have been placed in operation at the user entity:

Control Objective	Complementary User Entity Controls (CUECs)
CO1 - Organization and Administration: Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Cloud Platform System.
	Customers are responsible for providing the appropriate training to end-users on proper use of the Google Cloud Platform System consistent with the Acceptable Use Policies and Terms of Service. Acceptable Use Policies available at (or such URL as Google may provide): • Google Cloud Platform: https://cloud.google.com/terms/aup • Chronicle (Security Product) and Threat Intelligence for Chronicle: https://chronicle.security/legal/service-terms/
	Customers are responsible for ensuring that end-users are trained on the organizational policies and procedures relevant to the use of the Google Cloud Platform System.
	Customers are responsible for defining, documenting, and making available to users procedures for the operation of their instance of the Google Cloud Platform System.
	Customers are responsible for identifying and managing the inventory of information assets on the Google Cloud Platform System.
	Customers are responsible for establishing organizational policies and procedures for the use or integration of third-party services.

Control Objective	Complementary User Entity Controls (CUECs)
	Customers are responsible for reviewing the information security policies and the security capabilities in the Google Cloud Platform System to determine their applicability and modify their internal controls as appropriate.
	Customers are responsible for establishing documented policies and procedures for the transfer and sharing of information within their organization and with third-party entities.
CO2 - Logical Access: Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.	Customers are responsible for assigning responsibilities for the operation and monitoring of the Google Cloud Platform System.
	Customers are responsible for 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 defining and maintaining policies and procedures governing the customer's administration of access to the Google Cloud Platform System.
	Customers are responsible for provisioning service availability, user roles, and sharing permissions within the Google Cloud Platform System consistent with customer organizational policies.
	Customers are responsible for implementing secure log-on procedures to access the Google Cloud Platform System 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.

Control Objective	Complementary User Entity Controls (CUECs)
	Customers are responsible for enabling and enforcing the use of two-step verification on privileged administrator accounts.
	Customers are responsible for establishing procedures to allocate the initial password to access the Google Cloud Platform System to end-users when Google password authentication is used.
	Customers are responsible for training users on the use and disclosure of passwords used to authenticate to the Google Cloud Platform System.
	Customers are responsible for configuring GCP Marketplace permissions in Google Cloud Platform consistent with customer's internal policies (GCP Marketplace contains enterprise applications that can be added to a Google Cloud Platform).
	Customers are responsible for restricting access to and monitoring the use of Application Programming Interfaces (APIs) available in the Google Cloud Platform System.
	Customers are responsible for configuring domain settings related to integration with other systems within the customer's environment consistent with customer policies.
	Customers are responsible for configuring the Google Cloud Platform System mobile device options consistent with customer policies and procedures.
	Customers are responsible for the deployment, configuration and modification of default security settings for cloud products including virtual machines in accordance with their information security requirements.
CO3 - Change Management: Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.	Customers are responsible for ensuring any application software which they deploy onto the Google Cloud Platform System follows their specific software change management policies and procedures.
	Customers are responsible for training, testing, and deploying AI models that are used in AI-powered applications.

Control Objective	**Complementary User Entity Controls (CUECs)**
	Customers are responsible for periodically reviewing the configuration of the Google Cloud Platform System to ensure it is consistent with their policies and procedures.
	Customers are responsible for ensuring that user data is exported and deleted from the Google Cloud Platform System before or within a reasonable amount of time after termination.
	Customers are responsible for ensuring that individuals creating and/or updating profiles or changing the product configurations are authorized.
	Customers are responsible for reviewing and testing features, builds, and product releases, including Application Programming Interfaces (APIs), to evaluate their impact prior to deploying into production environments, as applicable.
	Customers are responsible for configuring test and/or development environments in their instance of the Google Cloud Platform System, as applicable, and restricting access to data in these environments.
	Customers are responsible for managing and testing configurations that support their business and operational resiliency objectives, and for considering Google Cloud Platform architecture recommendations.
CO4 - Physical Security: Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.	Customers are responsible for ensuring appropriate physical security controls over all devices that access the Google Cloud Platform System.
	Customers are responsible for ensuring any devices that access the Google Cloud Platform System or contain customer data are properly handled, secured, and transported as defined by the products requirements.
CO5 - Incident Management: Controls provide reasonable assurance that application and system incidents are identified,	Customers should train administrators and end-users on their responsibilities and organizational procedures for identifying, handling, and responding to security incidents pertaining to the use of the Google Cloud Platform System.

Control Objective	Complementary User Entity Controls (CUECs)
recorded, tracked, and resolved in a complete and timely manner.	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.
	Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Cloud Platform System.
CO6 - Availability: Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.	Customers are responsible for ensuring they have business recovery and backup procedures over their non-Google managed information systems that access the Google Cloud Platform System.
	Customers are responsible for configuring data storage locations that support their business and operational resiliency requirements.

SECTION IV - Description of Control Objectives, Controls, Tests and Results of Tests

Description of Control Objectives, Controls, Tests and Results of Tests

Testing performed and results of tests of entity level controls

In planning the nature, timing and extent of our testing of the controls specified by Google LLC, we considered the aspects of Google's control environment, risk assessment process, communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Sample sizes were selected using based on the nature of the control (e.g., automated or manual), the frequency of the control, and the available population.

Google centrally manages the majority of the controls from their headquarters in Mountain View, CA. However, certain physical security controls are operated at the individual data centers as listed in the system description. To help ensure controls are consistently designed and implemented across the data centers, the data center security team performs a review of each data center annually that is reviewed and approved by Google management. We perform site visits of the data centers on a rotation schedule to corroborate, through independent procedures (including observation and inspection), the controls are implemented as described within Google's review. We designed the visit schedule to ensure that each data center is visited at least once every three years and that new in-scope data centers are visited in the period they are brought into scope.

Control objectives and related controls for systems and applications

On the pages that follow, the applicable control objectives and the controls to achieve the objectives have been specified by, and are the responsibility of, Google LLC. The sections "Tests Performed by EY" and "Results" are the responsibility of Ernst & Young LLP.

For tests of controls requiring the use of Information Produced by the Entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), EY performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the IPE, (2) inspected the query, script, or parameters used to generate the IPE, (3) tied data between the IPE and the source, and/or (4) inspected the IPE for anomalous gaps in sequence or timing to determine the data was complete, accurate, and maintained its integrity. Furthermore, in addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings); we inspect management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
1. Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.
	Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
	Inspected a sample of launches and determined a design document and privacy review were completed prior to the launch.	No deviations noted.
	Inspected a sample of official product blogs for system changes and determined relevant personnel and impacted customers were notified.	No deviations noted.
2. The organization tests, validates, and documents changes to its services prior to deployment to production.	Inquired of the Program Manager and determined that application and configuration changes are tested, validated, and documented prior to deployment to production.	No deviations noted.
	Inspected the associated ticket details for a sample of Google Cloud Platform application and configuration changes in the code management system and determined that the changes were tested, validated, and documented prior to implementation to production.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
3. The organization has implemented a formal reporting structure that is made available to personnel.	Inquired of the Program Manager and determined the organization implemented a formal reporting structure that was made available to personnel.	No deviations noted.
	Inspected the organization's intranet and determined organizational charts showing formal reporting structure were made accessible to employees and included drill-down functionality to identify employees within the organizational structure, including employees in their functional teams.	No deviations noted.
	Inspected a sample communication and determined top level management changes were communicated internally and externally.	No deviations noted.
	Inspected the meeting minutes of a sample Board of Directors forum and determined management considered requirements such as integrity and security when defining authorities, structures, reporting lines, and responsibilities.	No deviations noted.
	Inspected procedural documents and determined management planned and prepared for succession by developing contingency plans for assignments of responsibility.	No deviations noted.
4. The organization notifies customers of updates to its confidentiality guidelines, objectives, and practices.	Inquired of the Program Manager and determined the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected the organization's Terms of Service and determined the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.
	Inspected GCP's customer documentation and determined that the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.
5. The organization performs privacy reviews prior to product launch.	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.
	Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
	Inspected a sample of launches and determined a design document and privacy review were completed prior to the launch.	No deviations noted.
	Inspected a sample of official product blogs for system changes and determined relevant personnel and impacted customers were notified.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
6. Company goals and responsibilities are required to be developed and communicated by management on a periodic basis, and amended as needed. Results are evaluated and communicated to employees.	Inquired of the Program Manager and determined company goals and responsibilities were developed and communicated by management and amended as needed. Results of the annual goals were evaluated and communicated to employees.	No deviations noted.
	Inspected a sample of goals and responsibilities and determined they were developed and evaluated by management.	No deviations noted.
	Inspected a sample of announcements and determined results of previous goals were communicated to employees.	No deviations noted.
7. The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Inquired of the Program Manager and determined Google published its commitments to security, availability, processing integrity and confidentiality to external users via Terms of Service (ToS).	No deviations noted.
	Inspected Google Cloud Platform's Terms of Service and product websites and determined Google's commitments to security, availability, processing integrity, and confidentiality are published for external users.	No deviations noted.
8. The descriptions of the organization's systems (including their scope and	Inquired of the Program Manager and determined that descriptions of the organization's systems, including their scope and boundaries, were made available to internal teams.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
boundaries) are made available to internal teams.	Inspected the internal website for all internal products and determined a description of the organization's system and its boundaries were available to the organization's internal product teams.	No deviations noted.
	Inspected the internal product website and determined a description of the organization's system and its boundaries were available to the organization's internal product teams.	No deviations noted.
9. Descriptions of the organization's system and its boundaries are available to external parties via ongoing communications with customers or via its official blog postings.	Inquired of the Program Manager and determined descriptions of the organization's system and its boundaries were available to authorized external users via ongoing communications with customers or via its official blog postings.	No deviations noted.
	Inspected the organization's official blog postings and determined descriptions of the organization's system and its boundaries were communicated.	No deviations noted.
10. Customer responsibilities are described on the organization's product websites or in system documentation.	Inquired of the Program Manager and determined customer responsibilities were described on product websites or in system documentation.	No deviations noted.
	Inspected the GCP website or in system documentation accessible by external customers and determined customer responsibilities were described.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
11. The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.	Inquired of the Program Manager and determined privacy and information security training program was in place and relevant personnel were required to complete this training annually.	No deviations noted.
	Inspected internal documentation and determined privacy and information security training program was in place and relevant personnel were required to complete the training annually.	No deviations noted.
	Inspected a sample email notification sent to Google personnel and determined reminders were sent to complete the privacy and information security training within a specified time.	No deviations noted.
	Inspected the completion rate for the privacy and information security training for Google personnel and determined relevant personnel completed the trainings in the last 12 months or were actively being monitored until completion of training.	No deviations noted.
	Inspected the privacy and information security training material and determined that Google has outlined the importance of information security and maintaining user, customer and employee privacy.	No deviations noted.
	Inspected the continuing education documents and determined that the entity provided training programs to help ensure skill sets and technical competencies of existing employees and contractors were developed and maintained.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected the training activity dashboard and determined that the privacy and information security training was mandatory and required to be completed annually.	No deviations noted.
12. The organization develops and maintains a risk management framework to manage risk to an acceptable level.	Inquired of the Program Manager and determined the organization developed and maintained a risk management framework to manage risk to an acceptable level.	No deviations noted.
	Inspected the vulnerability management and severity guidelines and determined a risk management framework was developed and documented to manage risk to an acceptable level, defined resolution time frames for risks, and to consider the potential for fraud.	No deviations noted.
	Inspected internal documentation and determined the organization maintains a security risk assessment framework to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented and signed off by management.	No deviations noted.
	Inspected the organization's risk assessment and determined the organization evaluates qualitative and quantitative factors to identify residual risk in order to manage risk to an acceptable level.	No deviations noted.
	Inspected meeting invites and relevant documentation from the organization's annual risk assessment discussion and determined the organization's operational objectives, potential impacts, and changes to the business model were considered.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected the internal insider risk site and determined the organization considered insider risk in its risk management framework to manage risk to an acceptable level.	No deviations noted.
13. The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inquired of the Program Manager and determined the organization had a vulnerability management program in place to detect and remediate system vulnerabilities.	No deviations noted.
	Inspected internal policies and guidelines and determined the organization had a vulnerability management program in place to identify, detect, report, prioritize, and remediate system vulnerabilities.	No deviations noted.
	Inspected internal documentation and determined vulnerabilities were classified based on the priority level.	No deviations noted.
	Inspected relevant configurations and determined vulnerabilities were tracked through an internal ticketing system as outlined in the vulnerability management program.	No deviations noted.
	Inspected a sample of identified vulnerabilities and determined they were tracked in an internal ticketing system through remediation.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
14. The organization requires external parties (Service Providers) to meet security and privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	Inquired of the Program Manager and determined the organization required external parties (Service Providers) to meet security and privacy requirements for safeguarding user data and the requirements were enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for providers and partners, respectively.	No deviations noted.
	Inspected the Third-Party Data Protection internal site and determined the organization had a formal due diligence process in place for engaging with third parties.	No deviations noted.
	Inspected the Information Protection Addendum (IPA) template and determined appropriate information security and data protection terms were documented within the IPA.	No deviations noted.
	Inspected the Partner Information Protection Addendum (PIPA) template and determined appropriate information security and data protection terms were documented within the PIPA.	No deviations noted.
	Inspected a sample Vendor that processess Google customer data and determined that they had signed an Information Protection Addendum (IPA) or Partner Information Protection Addendum (PIPA)	No deviations noted.
15. Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and	Inquired of the Program Manager and determined security and privacy policies are reviewed at least annually, and supporting standards, guidelines, and FAQs are created and updated as needed.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
FAQs are created and updated as needed.	Inspected internal documentation and determined that security and privacy policies, supporting standards, guidelines and FAQS were in place.	No deviations noted.
	Inspected internal documentation and determined security and privacy policies were reviewed at least annually and authorized before they were implemented.	No deviations noted.
	Inspected the most recent security and privacy policy reviews and determined policies were approved by authorized personnel or committee, reviewed at least annually, and updated as needed.	No deviations noted.
16. The organization has an established Internal Audit function which evaluates management's compliance with security controls.	Inquired of the Program Managers and Internal Audit and determined that the organization had an established internal compliance function which evaluated management's compliance with security, identity, authentication, and source code management controls.	No deviations noted.
	Inspected evaluations performed by the internal compliance function for a sample of semiannual periods and determined that the compliance function performed an evaluation of management's compliance with security, identity, authentication, and source code management controls.	No deviations noted.
	Inspected evaluations performed by management for a sample of quarters and determined that management performed an evaluation of their compliance with security, identity, authentication, and source code management controls.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected the meeting invites related to Google's annual organizational risk assessment and determined that the company's operational objectives, and potential impacts and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.
17. The organization periodically reviews and validates the design, operation and control record of in-scope compliance controls.	Inquired of the Program Managers and Internal Audit and determined the organization had an established internal compliance function which evaluated management's compliance with security, identity, authentication, and source code management controls.	No deviations noted.
	Inspected evaluations performed by the internal compliance function for a sample of semiannual periods and determined the compliance function performed an evaluation of management's compliance with security, identity, authentication, and source code management controls.	No deviations noted.
	Inspected evaluations performed by management for a sample of quarters and determined management performed an evaluation of their compliance with security, identity, authentication, and source code management controls.	No deviations noted.
	Inspected the meeting invites related to Google's annual organizational risk assessment and determined company's operational objectives, and potential impacts and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
18. The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inquired of the Program Manager and determined the organization conducted periodic information security risk assessments to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No deviations noted.
	Inspected applicable documentation and determined a risk management framework was developed and documented to manage risk to an acceptable level and defined resolution time frames for risks.	No deviations noted.
	Inspected the risk assessment and determined the organization conducted periodic information security risk assessments and identified, evaluated and mitigated risks to acceptable levels based on risk criteria, which are established, documented and approved by management.	No deviations noted.
	Inspected the organization's risk assessment and determined management signed off on the annual risk assessments performed.	No deviations noted.
19. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by management.	Inquired of the Program Manager and determined the organization conducted periodic information security risk assessments to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No deviations noted.
	Inspected internal documentation and determined management signed off on the risk management framework.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected the organization's risk assessment and determined the organization evaluates qualitative and quantitative factors to identify residual risk in order to manage risk to an acceptable level.	No deviations noted.
20. The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inquired of the Program Manager and determined the organization requires its employees to sign confidentiality agreements that define responsibilities and expected behavior for the protection of information.	No deviations noted.
	Inspected a sample of confidentiality agreements and determined they defined employee responsibilities and expected behavior for the protection of information.	No deviations noted.
	Inspected a sample of Google employees and determined they signed confidentiality agreements as part of their employment conditions.	No deviations noted.
21. The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	Inquired of the Program Manager and determined the organization established a disciplinary process to address non-compliance with company policies, code of conduct, or other personnel requirements.	No deviations noted.
	Inspected internal documentation and determined the organization established a disciplinary process for non-compliance with the company policies, code of conduct, or other personnel requirements which could result in dismissal, lawsuits and/or criminal prosecution.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected the disciplinary procedures undertaken for sample incidents and determined appropriate action was taken in cases of non-compliance with company policies, code of conduct, or other personnel requirements.	No deviations noted.
22. Personnel of the organization are required to acknowledge the code of conduct.	Inquired of the Program Manager and determined employees and extended workforce personnel were required to acknowledge the Code of Conduct as part of the terms and conditions of employment.	No deviations noted.
	Inspected internal documentation and determined employees and extended workforce personnel were required to acknowledge the Code of Conduct as part of the terms and conditions of employment.	No deviations noted.
	Inspected a sample of newly hired employees and extended workforce personnel and determined the Code of Conduct was acknowledged as part of the terms and conditions of their employment.	No deviations noted.
23. New hires or internal transfers are required to go through an official recruiting process during which they are screened against detailed job descriptions and interviewed to assess competence.	Inquired of the Program Manager and determined that new hires and internal transfers were required to go through an official recruiting process during which their qualifications and experience were screened to help ensure that they were competent to fulfill their responsibilities.	No deviations noted.
	Inspected a sample of new hires and internal transfers and determined positions had detailed job description including minimum and preferred qualifications, such as requisite skills and experiences , which candidates must meet in order to be hired.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected a sample of new hires and internal transfers and determined they went through a formal recruiting process and were screened against detailed job descriptions and interviewed to assess competence.	No deviations noted.
24. Background checks are performed on new hires as permitted by local laws.	Inquired of the Program Manager and determined background checks were performed for new hires as permitted by local laws.	No deviations noted.
	Inspected internal guidelines and determined background checks were part of the hiring process.	No deviations noted.
	Inspected a sample of new hires and determined background checks were performed as permitted by local laws.	No deviations noted.
25. The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inquired of the Program Manager and determined the organization had established agreements, including non-disclosure agreements, for preserving confidentiality of information and software exchanges with external parties, such as third-party vendors.	No deviations noted.
	Inspected the latest non-disclosure agreement template and determined the organization had established agreements with external parties for preserving confidentiality of information and software exchanges.	No deviations noted.
	Inspected agreements for a sample of external parties and determined the organization had signed non-disclosure agreements for preserving confidentiality of information and software exchanges with external parties.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
26. The Privacy, Safety Security Org (PSS) takes a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	Inquired of the Program Manager and determined that the Privacy, Safety Security Org (PSS) takes a risk based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	No deviations noted.
	Inspected the relevant documentation and determined the Security Engineering Org took a risk based approach to reviewing the security practices of vendors and the security posture of vendor products, including automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	No deviations noted.
	Inspected the security audit performed for a sample of vendors and determined the security practices of vendors and the security posture of vendor products were reviewed.	No deviations noted.
27. The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inquired of the Program Manager and determined the organization required its extended workforce personnel to sign confidentiality agreements that defined responsibilities and expected behavior for the protection of information.	No deviations noted.
	Inspected the Google confidentiality agreements and determined they defined extended workforce personnel responsibilities and expected behavior for the protection of information.	No deviations noted.

CO1 - Organization and Administration

Controls provide reasonable assurance that policies and procedures promote a corporate culture focused on integrity and security.

Control Description	Tests Performed by EY	Results
	Inspected a sample of Google extended workforce personnel and determined they signed the confidentiality agreements as part of their service conditions.	No deviations noted.
28. The organization has established a process to review and approve requests for policy exceptions.	Inquired of the Program Manager and determined the organization has a policy exception process to ensure a formal approval and risk evaluation are performed.	No deviations noted.
	Inspected applicable policies and determined the process to request and process policy exceptions was documented.	No deviations noted.
	Inspected a sample of policy exceptions and determined they followed the documented process.	No deviations noted.
29. The organization has policies and guidelines that govern the acceptable use of information assets.	Inquired of the Program Manager and determined the organization established policies and procedures that governed the acceptable use of information assets.	No deviations noted.
	Inspected the relevant documentation and determined Google established policies and procedures that governed the acceptable use of information assets.	No deviations noted.
30. 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.	Inquired of the Program Manager and determined confidentiality agreements for employees and third parties were in place, reviewed and updated as needed.	No deviations noted.
	Inspected the confidentiality agreements and determined they were reviewed and updated as needed by the organization.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
1. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	Inquired of the Program Manager and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
	Inspected internal policies regarding encryption mechanisms and determined the organization used encryption to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
	Inspected externally available documentation and determined the organization communicated how user authentication and administrator sessions transmitted over the Internet were encrypted.	No deviations noted.
	Inspected encryption mechanism documentation and configurations, and determined user authentication and administrator sessions transmitted over the Internet were encrypted.	No deviations noted.
	Observed connection settings to the organization's external websites for a user and an administrator and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
	Inspected the server scan results and determined the organization used encryption mechanisms to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
2. External system users are identified and authenticated via the Google Accounts or the BYOID authentication system before access is granted.	Inquired of the Program Manager and determined external system users were identified and authenticated via the Google Accounts authentication system before access is granted.	No deviations noted.
	Inspected the configuration supporting the login functionality and determined users were identified and authenticated via the Google Accounts authentication system before access was granted.	No deviations noted.
	Observed an external system user login with a valid Google account and determined access was granted.	No deviations noted.
	Observed an external system user attempt to login with an invalid Google account and determined access was denied.	No deviations noted.
3. 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.	Inquired of the Program Manager and determined access to sensitive systems and applications requires two-factor authentication in the form of user ID, password, security key, and/or certificate.	No deviations noted.
	Inspected the applicable policy and determined access to sensitive systems and applications required two-factor authentication in the form of user ID, password, security key and/or certificate.	No deviations noted.
	Inspected relevant policy documentation and determined Google has an established policy that specifies the use of emergency credentials.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the configuration and determined that personnel access to sensitive internal systems and applications required two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	No deviations noted.
	Observed a user attempt to gain access to a production machine with a valid user ID, password, security key, and certificate and determined access was granted.	No deviations noted.
	Observed a user attempt to gain access to a production machine without a valid certificate and determined access was not granted.	No deviations noted.
	Observed a user attempt to gain access to a production machine with valid emergency access credentials and determined access was granted.	No deviations noted.
	Observed a user attempt to gain access to a production machine without valid emergency access credentials and determined access was not granted.	No deviations noted.
	Inspect evidence to determine that the user who performed authentication to production using emergency access credentials had appropriate access approvals prior to obtaining access.	No deviations noted.
4. The organization has established formal guidelines for passwords to govern the	Inquired of the Program Manager and determined Google had established password guidelines to govern the management and use of authentication mechanisms.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
management and use of authentication mechanisms.	Inspected relevant documentation and determined formal guidelines for passwords were established to govern the management and use of authentication mechanisms.	No deviations noted.
	Inspected the relevant configurations and determined passwords were transmitted and stored in an encrypted manner.	No deviations noted.
	Inspected the password configurations propagated to servers and determined they were configured to enforce password requirements.	No deviations noted.
	Observed user attempt to login using incorrect password and determined the account was locked out after exceeding the maximum number of attempts allowed.	No deviations noted.
5. Mechanisms are in place to detect attempts, and prevent connections to the organization's network by unauthorized devices.	Inquired of the Program Manager and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
	Inspected relevant documentation and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
	Inspected relevant configurations and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Observed a user with an authorized device attempt to connect to the Google network and determined the connection was successful.	No deviations noted.
	Observed an unauthorized user attempt to connect to the Google network and determined access was denied.	No deviations noted.
	Observed a user attempt to connect to the production network with a valid certificate and determined the connection was successful.	No deviations noted.
	Observed a user attempt to connect to the production network without a valid certificate and determined that access was denied.	No deviations noted.
	Observed a user modify their certificate and determined that access was disconnected.	No deviations noted.
	Inspected a sample alert and determined mechanisms were in place to detect attempts at unauthorized connections to the organization's network.	No deviations noted.
6. Where "on demand request" mechanisms are implemented to restrict human access to production resources, access requests are reviewed and	Inquired of the Program Manager and determined that "on demand request" mechanisms were implemented to restrict human access to production resources, and "access on demand" requests are reviewed and approved by a second individual prior to being granted and the event is logged.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
approved by a second individual prior to being granted and the event is logged.	Inspected the documentation and determined that "access on demand" requests were reviewed and approved by an appropriate second individual prior to being granted and that the event was logged.	No deviations noted.
	Inspected the "access on demand" configuration supporting the functionality and determined access requests were configured to restrict human access to production resources via access groups and can only be granted for a limited number of hours.	No deviations noted.
	Observed an attempt to change the group membership default policy and determined changes were recorded and approved.	No deviations noted.
	Observed a user attempt to gain access to an on-demand group and determined access was granted after meeting the predefined conditions (i.e. authorized user request, appropriate approval from a second individual, limited number of hours).	No deviations noted.
	Observed a user attempt to gain access to an on-demand group and determined access was not granted when the predefined conditions (i.e. authorized user request, appropriate approval from a second individual, limited number of hours) were not met.	No deviations noted.
	Inspected a sample of system generated log and determined that on-demand group transactions were recorded.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
7. 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.	Inquired of the Program Manager and determined remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate.	No deviations noted.
	Inspected relevant documentation and determined remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificates.	No deviations noted.
	Inspected the remote access configuration and determined it required a Google issued digital certificate to be installed on the connecting device.	No deviations noted.
	Inspected the authentication settings for remote access to corporate machines and determined two-factor authentication was required.	No deviations noted.
	Observed a user attempt to gain remote access to corporate machine with a device that had a Google issued digital certificate installed and two-factor authentication and determined remote access to the corporate environment was successful.	No deviations noted.
	Observed a user attempt to gain remote access to corporate machine with a device that did not have a Google issued digital certificate installed or without two-factor authentication and determined remote access to the corporate environment was denied.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
8. Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	Inquired of the Program Manager and determined that access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	No deviations noted.
	Inspected relevant documentation and formal procedures for managing user access to production machines, support tools, and network devices via access control lists and determined that access requests and modifications must be recorded and approved by appropriate administrators.	No deviations noted.
	Inspected the configurations within the source code management system and determined that the relevant access control list systems were configured to enforce approval from a group administrator prior to a user receiving access to production machines, support tools, and network devices.	No deviations noted.
	Observed an attempt to grant user access to a group with the appropriate approval from the group administrator and determined access was granted.	No deviations noted.
	Observed an attempt to grant user access to a group without the appropriate approval from the group administrator and determined access was not granted.	No deviations noted.
	Inspected a sample of system generated logs for access to production machines, support tools, and network devices and determined access approvals and modifications to the access lists were recorded.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
9. Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.	Inquired of the Program Manager and determined access to the corporate network, which further provides access to production machines, network devices, and support tools, required a unique ID and verified credentials.	No deviations noted.
	Inspected the configuration for access to corporate network, network devices, production machines, and support tools and determined a unique ID and verified credentials were required.	No deviations noted.
	Observed a user attempt to create a user with a username belonging to another user and determined that a duplicate username could not be assigned.	No deviations noted.
	Observed a user attempt to create, delete, and recreate an account with the same username and determined the accounts were assigned unique IDs.	No deviations noted.
	Observed a user attempt to access the corporate network without verified credentials and determined access was denied.	No deviations noted.
	Observed a user attempt to access the corporate network with verified credentials and determined access was granted.	No deviations noted.
	Observed a user attempt to access the production machines with an authorized private key by using a valid SSH certificate and determined access was allowed.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Observed a user attempt to access the production machines without an authorized private key by using an invalid SSH certificate and determined access was denied.	No deviations noted.
	Observed a user attempt to obtain access to network devices after authenticating via user ID, password, security key, and/or certificate and determined that the user successfully obtained access.	No deviations noted.
	Observed a user attempt to obtain access to network devices without first authenticating via user ID, password, security key, and/or certificate and determined that the user failed to obtain access.	No deviations noted.
	Observed a user attempt to access an internal support tool with approved credentials and determined access was granted.	No deviations noted.
	Observed a user attempt to access an internal support tool without approved credentials and determined access was not granted.	No deviations noted.
10. Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis	Inquired of the Program Manager and determined access to production machines, support tools, network devices and corporate assets was automatically removed in a timely basis upon submission of a termination request by Human Resources or a manager.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
upon submission of a termination request by Human Resources or a manager.	Inspected relevant documentation and determined requirements for terminating users with access to production machines, support tools, network devices and corporate assets were documented.	No deviations noted.
	Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined it was configured to remove access upon submission of a termination request by Human Resources or a manager.	No deviations noted.
	Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined that any failures in the process will generate an alert.	No deviations noted.
	Inspected a sample alert from the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined that the failure was resolved in a timely manner.	No deviations noted.
	Inspected a sample of terminated users and determined that access to production machines, support tools, network devices, and corporate assets was automatically revoked by the automated tool within seven (7) days of the user's termination date.	No deviations noted.
11. Only users with a valid user certificate, corresponding private key and appropriate authorization (per host) can	Inquired of the Program Manager and determined only users with a valid certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
access production machines via SSH.	Inspected relevant documentation and determined mechanisms are in place to authenticate users and restrict access to production machines without a valid digital certificate.	No deviations noted.
	Inspected the configuration enforcing authorized key authentication and determined it was set up to restrict access to production machines from unauthorized users without a valid digital certificate.	No deviations noted.
	Inspected the configuration that enforced the authentication of users prior to granting a private key and determined digital certificates were only generated after a user was authenticated using two-factor authentication.	No deviations noted.
	Observed a user attempt to access the production machines with an authorized private key by using a valid SSH certificate and determined access was allowed.	No deviations noted.
	Observed a user attempt to access the production machines without an authorized private key by using an invalid SSH certificate and determined access was denied.	No deviations noted.
12. The organization has a security guideline that requires users to lock their workstations and mobile devices when unattended. Workstations are configured to initiate a	Inquired of the Program Manager and determined a security guideline was in place that required users to lock workstations and mobile devices when unattended.	No deviations noted.
	Inspected internal policies and determined the organization required users to lock their workstations and mobile devices when unattended.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
password protected screen-saver after 15 minutes of inactivity (i.e., no input from device user).	Inspected the idle time configurations propagated to workstations and determined they were configured to enforce password standards.	No deviations noted.
	Performed on-site inspections for a sample of offices and determined that employees followed appropriate office security practices including locking workstations when unattended.	No deviations noted.
	Observed a sample of corporate machines and determined users were locked out after reasonable amount of time of inactivity.	No deviations noted.
13. Security event logs are protected and access is restricted to authorized personnel.	Inquired of the Program Manager and determined security event logs were protected and access was restricted to authorized personnel.	No deviations noted.
	Inspected the system configuration related to audit logs and determined log files were not modifiable.	No deviations noted.
	Inspected internal documentation and determined policies and procedures for restriction of logical access to audit logs to authorized personnel were in place.	No deviations noted.
	Inspected a sample of members with access to audit logs and determined they were appropriate to have access to audit logs.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected a sample semiannual user access review and determined access to audit logs was reviewed on a periodic basis and that appropriate action was taken to resolve inappropriate access, if applicable.	No deviations noted.
14. Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.	Inquired of the Program Manager and determined access to network devices was authenticated via user ID, password, security key, and/or certificate.	No deviations noted.
	Inspected the access configuration for production network devices and determined it required authentication via user ID, password, security key, and/or certificate.	No deviations noted.
	Observed a user attempt to obtain access to network devices after authenticating via user ID, password, security key, and/or certificate and determined that the user successfully obtained access.	No deviations noted.
	Observed a user attempt to obtain access to network devices without first authenticating via user ID, password, security key, and/or certificate and determined that the user failed to obtain access.	No deviations noted.
15. The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inquired the Program Manager and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
	Inspected the policies and documents related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the configurations related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
16. Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	Inquired of the Program Manager and determined access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No deviations noted.
	Observed a user attempt to access an internal support tool with approved credentials and determined access was granted.	No deviations noted.
	Observed a user attempt to access an internal support tool without approved credentials and determined access was not granted.	No deviations noted.
17. Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Inquired of the Program Manager and determined that critical access groups were reviewed periodically by group administrators.	No deviations noted.
	Inspected relevant documentation and determined that critical access group reviews were done on a periodic basis and scoping was determined accordingly.	No deviations noted.
	Inspected the code configuration and determined that tools used to facilitate the review generate complete and accurate critical access group listings.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected a sample of critical access group user membership reviews performed by the appropriate group administrator and determined the review was performed in a timely manner.	**Deviation noted.** Four (4) of 25 critical access groups in the semi-annual review sampled for testing were not performed timely.
	Management's Response: Management acknowledges that the periodic access reviews for 4 selected critical access groups were not performed in a timely manner and completed after the defined service level objective (SLO). Although the critical access group review control process is common across different Google products, management identified that one (1) of the 4 critical access reviews was related to a Google Cloud product and was identified in H2 2023. The remaining 3 critical access reviews were not related to Google Cloud products and were identified in H1 2024 Management reviewed the memberships to the access groups and determined that there was no inappropriate access identified as result of the delayed reviews. Management has reiterated the importance of timely completion of the user access reviews to the relevant teams to ensure that reviews are completed within the defined SLO.	
	Inspected a sample of users from the review of critical access groups and determined their access was appropriate based on their cost center.	No deviations noted.
	Inspected a sample of critical access group user membership reviews and determined that appropriate action was taken to resolve inappropriate access identified, if applicable.	No deviations noted.

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected a sample of critical access group reviews and determined they reviewed a complete and accurate listing of critical access groups.	**Deviation noted.** Four (4) of 13 products sampled as part of testing the critical access groups identified by management as having access to approve automated releases of changes, were not reviewed during the audit period.
	Management's Response: Management acknowledges that critical access groups for four (4) sampled products were not included in the periodic access review process. Although the critical access group review control process is common across different Google products, management identified that one (1) of the 4 critical access groups was related to a Google Cloud product. The remaining 3 critical access groups were not related to Google Cloud products. These omissions were a result of a manual error. Management reviewed the memberships to the access groups and determined that there was no inappropriate access and that memberships to the group had annual auto-expiration implemented. The access groups have since been added to the periodic access review process. Furthermore, management reviewed the end-to-end release process for the selected products and determined that the release process was automated with no access to human users. The individuals within the identified groups were responsible for providing a second layer of approval before software binaries for the related product could be released to production. As a result of the review, management has determined that there was no impact to production systems and that the deviation has been remediated.	

CO2 - Logical Access

Controls provide reasonable assurance that logical access to production systems and data is restricted to authorized personnel.

Control Description	Tests Performed by EY	Results
18. The organization uses encryption to secure user data in transit between the organization's production facilities.	Inquired of the Program Manager and determined encryption is used to secure user data in transit between the organization's production facilities.	No deviations noted.
	Inspected internal documentation and determined encryption is used to secure user data in transit between the organization's production facilities.	No deviations noted.
	Inspected the encryption configuration and determined encryption is used to secure user data in transit between the organization's production facilities.	No deviations noted.
19. The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	Inquired of the Program Manager and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	No deviations noted.
	Inspected the internal documentation and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the network	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
1. Development, testing and build environments are separated from the production environment through the use of logical security controls.	Inquired of the Program Manager and determined the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
	Inspected internal documentation and determined the organization maintained separate development, testing, and production environments.	No deviations noted.
	Inspected applicable code repository branch protection rules and determined the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
	Inspected a sample Google Cloud Platform change and determined the organization separated development, testing, and build environments from production through the use of logical security controls.	No deviations noted.
	Inspected a sample of products and determined access to deploy changes to production was restricted to appropriate individuals.	No deviations noted.
2. Changes to customer facing services that may affect confidentiality, processing integrity and / or availability are communicated to relevant	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
personnel and impacted customers.	Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
	Inspected a sample of launches and determined a design document and privacy review were completed prior to the launch.	No deviations noted.
	Inspected a sample of official product blogs for system changes and determined relevant personnel and impacted customers were notified.	No deviations noted.
3. Changes to the organization's systems are tested before being deployed.	Inquired of the Program Manager and determined that application and configuration changes are tested, validated, and documented prior to deployment to production.	No deviations noted.
	Inspected the associated ticket details for a sample of Google Cloud Platform application and configuration changes in the code management system and determined that the changes were tested, validated, and documented prior to implementation to production.	No deviations noted.
4. The organization uses a version control system, to manage source code, documentation, release	Inquired of the Program Manager and determined the organization used an internal code management system to manage source code, documentation, release labeling, and that access to the system has to be approved.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
labeling, and other functions. Access to the system must be approved.	Inspected internal documentation and determined the organization uses a version control system, to manage source code, documentation, release labeling, and other functions.	No deviations noted.
	Inspected code change management tools and determined that there was a version control system in place to manage source code, code documentation, and release labeling.	No deviations noted.
	Inspected the system configurations for the code management system and determined the system was configured to require an approval prior to granting access to the version control system.	No deviations noted.
5. System changes are reviewed and approved by a separate technical resource before moving into production.	Inquired of the Program Manager and determined the organization used an approved code management system to manage source code, documentation, release labeling, and that access to the system has to be approved.	No deviations noted.
	Inspected the applicable code for the organization's code management system and determined system changes required a review by a separate technical resource before migration to production.	No deviations noted.
	Inspected evidence of transaction testing made by a user to the version code management system and determined that it required changes to be reviewed by a separate technical resource before migration to production.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
6. The organization has established guidelines for governing the installation of software on organization-owned assets.	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
	Inspected Google's security policies and determined Google had implemented rules to govern the installation of software by users.	No deviations noted.
	Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
	Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
	Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.
7. A standard image is utilized for the installation and maintenance of each production server.	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
	Inspected Google's security policies and determined Google had implemented rules to govern the installation of software by users.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
	Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
	Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Inspected the relevant user groups and determined access to deploy software was restricted to authorized engineers.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
8. Integrity checks are in place at the file system level to ensure data integrity.	Inquired of the Program Manager and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.
	Inspected the organization's security policies and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.
	Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations to ensure data integrity at the file system level.	No deviations noted.
	Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration to ensure data integrity at the file system level.	No deviations noted.
	Observed a Software Engineer insert a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
	Observed a Software Engineer modify a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
	Observed a Software Engineer delete a sample file in the directory of a haphazardly selected production machine and determined the tool detected the deleted sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
9. Changes to network configurations are reviewed and approved prior to deployment.	Inquired of the Program Manager and determined changes to network configurations were reviewed, approved, and tested prior to deployment.	No deviations noted.
	Inspected a sample of manual network configuration changes and determined they were reviewed by a separate technical resource to validate quality and accuracy.	No deviations noted.
	Inspected a sample of manual network configuration changes and determined they were tested prior to deployment.	No deviations noted.
	Inspected a sample automated change and determined it was made by an automated tool based on the pre-configured ruleset.	No deviations noted.
	Inspected a sample change made to the automated tool and determined it was reviewed by a separate technical resource to validate quality and accuracy and tested prior to deployment.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
10. Mobile code is blocked by default via standard (Chrome) web browser configurations on company owned endpoints.	Inquired of the Program Manager and determined mobile code (code that is executed in a remote location) is blocked by default via standard web browser configurations on Google workstations and laptops.	No deviations noted.
	Inspected relevant documents and policies for configuration of the standard web browser (Chrome) on Google workstations and laptops and determined the organization implemented rules to restrict unauthorized portable code.	No deviations noted.
	Inspected relevant code configurations and determined rules were configured to block code via standard web browser (Chrome) configurations.	No deviations noted.
	Observed a standard web browser (Chrome) and determined blocked extensions/domains could not be accessed.	No deviations noted.
11. Integrity checks are in place at the application level to ensure data integrity.	Inquired of the Program Manager and determined integrity checks were in place via checksum verifications at the application level to help ensure data integrity.	No deviations noted.
	Inspected application level configurations and determined they were configured to use integrity checks via checksum verification.	No deviations noted.
	Observed a user attempt to upload files to a sample application and determined application level integrity checks via checksum verification were in place to help ensure data integrity.	No deviations noted.

CO3 - Change Management

Controls provide reasonable assurance that changes to applications and infrastructure are properly tested, documented, code reviewed, and implemented by authorized personnel.

Control Description	Tests Performed by EY	Results
12. The organization has policies and guidelines governing the secure development lifecycle.	Inquired of the Program Manager and determined the organization had policies and procedures which govern the secure development lifecycle.	No deviations noted.
	Inspected internal documentation and determined the organization had policies and procedures which govern the secure development lifecycle.	No deviations noted.
13. The organization has a published policy about retention and deletion of user data.	Inquired of the Program Manager and determined Google had a User Data Retention and Deletion Policy.	No deviations noted.
	Inspected the User Data Wipeout Policy and other related documentation, and determined it established guidelines to govern the retention and deletion of user data.	No deviations noted.
14. The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Inquired of the Program Manager and determined change management policies, including security code reviews, were in place, and procedures for tracking, testing, approving, and validating changes were documented.	No deviations noted.
	Inspected internal policies and determined practices for security code review, tracking, testing, approving, and validating changes were documented.	No deviations noted.

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
1. Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	Inquired of the Data Center Facilities Manager and determined that physical security measures were in place as described and are reviewed through the annual data center security review.	No deviations noted.
	Inspected a sample data center security review performed for the production facilities and determined that management reviewed the physical security measures at the facilities.	No deviations noted.
	Observed a sample of data centers and determined that visitors obtained approvals from authorized personnel prior to their visits, had their identities verified before entering the data center floors, and remained with an escort during the duration of their visits.	No deviations noted.
	Observed a sample of data centers and determined that data centers were continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	No deviations noted.
	Observed a sample of data centers and determined that data centers were secured through the use of badge reader and biometric control systems.	No deviations noted.
	Inspected the badge reader activity logs for a sample of data centers and determined access to Google spaces was logged and monitored.	No deviations noted.

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Inspected the badge reader activity logs for a sample of data centers and determined logs were retained for at least 3 months.	No deviations noted.
2. Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	Inquired of the Operations Manager and determined information systems and equipment were safeguarded against unauthorized entry and removal from data centers and data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	No deviations noted.
	Inspected internal documentation and determined that the organization maintains policies and guidelines around the security of storage devices during delivery and movement throughout the data center.	No deviations noted.
	Observed a sample of data centers and determined that Google had safeguards in place to protect information systems and equipment from unauthorized entry and removal from data centers.	No deviations noted.
	Observed a sample of data centers and determined that dedicated receiving and shipping areas were isolated from the main data center floor, network rooms and security systems.	No deviations noted.
	Inspected a sample of tickets created for data center equipment entering and exiting data centers and determined Google authorized, monitored, and controlled the shipments and maintained a record of the items.	No deviations noted.

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
3. The organization authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items.	Inquired of the Operations Manager and determined information systems and equipment were safeguarded against unauthorized entry and removal from data centers and data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	No deviations noted.
	Inspected internal documentation and determined that the organization maintains policies and guidelines around the security of storage devices during delivery and movement throughout the data center.	No deviations noted.
	Observed a sample of data centers and determined that Google had safeguards in place to protect information systems and equipment from unauthorized entry and removal from data centers.	No deviations noted.
	Observed a sample of data centers and determined that dedicated receiving and shipping areas were isolated from the main data center floor, network rooms and security systems.	No deviations noted.
	Inspected a sample of tickets created for data center equipment entering and exiting data centers and determined Google authorized, monitored, and controlled the shipments and maintained a record of the items.	No deviations noted.

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
4. Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.	Inquired of the Program Manager and determined user access to high-security areas in data centers was reviewed on a quarterly basis and inappropriate access was removed in a timely manner.	No deviations noted.
	Inspected the internal policies and determined user access to high-security areas in data centers was reviewed on a periodic basis.	No deviations noted.
	Inspected a sample of quarterly data center access reviews and determined that reviews were performed completely and accurately in a timely manner by appropriate personnel.	No deviations noted.
	Inspected a sample of users marked as appropriate within a quarterly data center access review and determined the users were appropriate based on cost center and job title.	No deviations noted.
	Inspected a sample of inappropriate users identified as requiring removal within a quarterly data center access review and determined the users were removed in a timely manner.	No deviations noted.
5. Redundant power is utilized to support the continued operation of critical data center equipment in the event of a	Inquired of the Data Center Operations Manager and determined redundant power was utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power sources.	No deviations noted.

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
loss of the primary power source(s).	Observed a sample of data centers and determined that network rooms were connected to an UPS system and emergency generator power was available for at least 24 hours in the event of a loss of power.	No deviations noted.
	Observed a sample of data centers and determined that data centers were equipped with redundant network connections via different physical connections.	No deviations noted.
	Inspected maintenance records for in-scope data centers and observed that equipment was continuously monitored and periodically tested.	No deviations noted.
6. Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.	Inquired of the Data Center Security Manager and determined visitors were required to gain approval from authorized personnel, have their identity verified and remain with an escort during the duration of their visit.	No deviations noted.
	Inspected the physical security policies and determined Google required visitors to gain approval from authorized personnel, have their identity verified at the perimeter and remain with an escort during the duration of their visit.	No deviations noted.
	Observed a sample of data centers and determined that individuals on-site had their identities verified before entering the data center floors.	No deviations noted.

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Inspected a sample of access requests to visit data centers and determined approvals were obtained from authorized personnel prior to the visits, and visitors remained with an escort during the duration of their visits.	No deviations noted.
7. Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.	Inquired of the Operations Manager and determined critical power and telecommunications equipment in data centers were physically protected from disruption and damage.	No deviations noted.
	Observed a sample of data centers and determined that power and telecommunications equipment in data centers were physically protected from disruption and damage.	No deviations noted.
	Observed a sample of data centers and determined that temperature and humidity of data halls were within the configured thresholds.	No deviations noted.
8. Automated mechanisms are utilized to track inventory of all production machines and inventory of all serialized server components.	Inquired of the Data Center Operations Manager and determined automated mechanisms were utilized to track inventory of production machines.	No deviations noted.
	Inspected the records from the inventory system for a sample of production machines selected during data center inspections and determined the selected machines existed in the inventory system.	No deviations noted.
	Observed a sample of production machines selected from the inventory system prior to the data center inspection and determined that the selected machines existed at the data centers.	No deviations noted.

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Inspected the records from the inventory system for a sample machine and determined that the selected machine and serialized components were tracked appropriately.	**Deviation noted.** For one (1) of the 23 sites sampled for testing, the status of one (1) destroyed drive sampled during the onsite visit, was not tracked appropriately from its storage through destruction.
	Management's Response: Management acknowledges and has reviewed the finding, noting the destroyed piece of storage media sampled by the external auditors for control testing was not part of the Google pool of production machines and that the control language is unclear as to the intended scope of applicability. Further, management has determined that sufficient protections are in-place and operational for storage media utilized to support production services (via policy enforcement engine and alerting mechanisms), the extent of impact for this observation is limited to storage media not utilized for production and not included in automated tracking/alerting solutions. Additionally, management will coordinate with the relevant teams to improve the specificity of control language to reduce likelihood of future confusion, and improve internal procedural documentation utilized by personnel performing audits or facilitating audits at data centers as to the potential presence/appropriate treatment for storage media utilized.	
9. Data centers are equipped with fire detection alarms and protection equipment.	Inquired of the Data Center Operations Facilities Manager and determined data centers were equipped with fire detection alarms and protection equipment.	No deviations noted.

CO4 - Physical Security

Controls provide reasonable assurance that physical access to computer equipment and other resources is restricted to appropriate personnel and that critical systems are protected from environmental threats and power interruptions.

Control Description	Tests Performed by EY	Results
	Observed a sample of data centers and determined that they were equipped with fire detection alarms and protection equipment.	No deviations noted.
	Observed a sample of data centers and determined that potential environmental threats to the data centers were anticipated and countermeasures were established based on the nature and geographical location of the data centers.	No deviations noted.
10. The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.	Inquired of the Data Center Security Manager and determined physical protection and guidelines were described in the Physical Security Policy, Data Security Policy, Google Photography Policy, and the Data Center Access policy.	No deviations noted.
	Inspected the Physical Security Policy, Data Security Policy, Google Photography Policy, and the Data Center Access Policy and determined that physical protection guidelines were specified within each document.	No deviations noted.
11. Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Inquired of the Program Manager and determined security measures utilized in data centers were assessed periodically and the results were reviewed by executive management.	No deviations noted.
	Inspected a sample of the reviews performed and determined security measures utilized in all data centers were assessed periodically and the results were reviewed by executive management.	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
1. The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inquired of the program manager and determined the organization provided monitoring tools to facilitate the detection and reporting of operational issues and the monitoring tools sent automated alerts to operational personnel based on predetermined criteria and are escalated per policy.	No deviations noted.
	Inspected relevant documentation and determined there were tools in place to detect and report operational issues to operational personnel.	No deviations noted.
	Inspected a sample of alerts and determined monitoring tools were in place to detect, report, escalate and resolve operational issues.	No deviations noted.
	Inspected evidence from an escalated sample security incident and determined appropriate action was taken to identify, record, track and resolve the incident in a timely manner.	No deviations noted.
2. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Inquired of the program manager and determined the organization provided monitoring tools to facilitate the detection and reporting of operational issues and the monitoring tools sent automated alerts to operational personnel based on predetermined criteria and are escalated per policy.	No deviations noted.
	Inspected relevant documentation and determined there were tools in place to detect and report operational issues to operational personnel.	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inspected a sample of alerts and determined monitoring tools were in place to detect, report, escalate and resolve operational issues.	No deviations noted.
	Inspected evidence from an escalated sample security incident and determined appropriate action was taken to identify, record, track and resolve the incident in a timely manner.	No deviations noted.
3. The organization provides external users with mechanisms to report security issues, incidents and concerns.	Inquired of the Program Manager and determined that the organization provides external users with mechanisms to report security issues, incidents, and concerns.	No deviations noted.
	Inspected the organization’s websites and determined mechanisms were available for external users to report security issues, incidents, and concerns.	No deviations noted.
	Inspected the organization's websites and determined separate communication channels were in place to enable anonymous or confidential communication when normal channels were inoperative or ineffective.	No deviations noted.
	Inspected a sample incident ticket raised by an external user through the established mechanisms to validate that the issue or concern was received by the organization.	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
4. Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
	Inspected Google's security policies and determined Google had implemented rules to govern the installation of software by users.	No deviations noted.
	Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
	Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
	Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
	Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.
5. The organization has a dedicated team responsible for managing security and privacy incidents.	Inquired of the Program Manager and determined the organization had a dedicated team responsible for managing security and privacy incidents involving security, availability, processing integrity and confidentiality, and provides internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.
	Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inspected relevant documentation and determined a process was in place for incident response teams to quantify, manage and monitor incidents.	No deviations noted.
	Observed the organization's incident management ticketing system and determined that mechanisms were in place to track internal and external reported security and privacy incidents through investigation and resolution.	No deviations noted.
	Inspected a sample of incident tickets and determined the incident response team quantified and monitored incidents.	No deviations noted.
6. Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Inquired of the Security Engineering Manager and determined audit logs were continuously monitored for events related to security, availability, processing integrity and confidentiality threats and alerts are generated for further investigation.	No deviations noted.
	Observed internal documentation and determined there are guidelines used by the Security Surveillance Team to classify, prioritize, perform cause analysis, and triage the security incidents.	No deviations noted.
	Observed internal documentation and determined the organization provides logging capabilities to its customers and customers can only access records related to their own activities.	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Observed a sample log configuration and determined log sources were monitored and maintained to continuously detect malicious or unusual insider activity.	No deviations noted.
	Observed a sample of alerts for events related to security, availability, processing integrity and confidentiality and determined alerts were generated when the pre-defined criteria was met.	No deviations noted.
	Observed the dashboard of monitoring tools and determined that alerts related to security, availability, processing integrity and confidentiality were monitored.	No deviations noted.
7. The organization has established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.	Inquired of the Program Manager and determined that the organization established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.	No deviations noted.
	Inspected relevant policies and guidelines and determined that the organization established a dedicated security team to engage in security and privacy of customer data.	No deviations noted.
	Inspected internal documentation and determined that a dedicated security team engaged in security and privacy of customer data managed security 24 x 7 worldwide.	No deviations noted.
	Inspected the on-call calendar configuration and determined that the on-call calendar was maintained according to a defined set of rules.	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inspected the on-call calendar configuration and determined that on-call rotation schedules were automated and any change in the schedule was subject to the management's approval process.	No deviations noted.
	Inspected the Incident Response team's on-call schedule and determined that the security team engaged in security and privacy was available 24 x 7.	No deviations noted.
8. The organization provides internal personnel (employees and extended workforce) with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	Inquired of the Program Manager and determined the organization had a dedicated team responsible for managing security and privacy incidents involving security, availability, processing integrity and confidentiality, and provides internal personnel with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	No deviations noted.
	Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.
	Inspected relevant documentation and determined a process was in place for incident response teams to quantify, manage and monitor incidents.	No deviations noted.
	Observed the organization's incident management ticketing system and determined that mechanisms were in place to track internal and external reported security and privacy incidents through investigation and resolution.	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
	Inspected a sample of incident tickets and determined the incident response team quantified and monitored incidents.	No deviations noted.
9. The organization maintains a framework that defines how to organize a response to security and privacy incidents.	Inquired of the Program Manager and determined the organization maintained a framework that defined how to organize a response to security and privacy incidents.	No deviations noted.
	Inspected the organization's internal incident response websites and determined incident response teams and procedures were established to handle security and privacy incidents.	No deviations noted.
	Inspected relevant documentation and determined a process was in place for incident response teams to quantify, manage and monitor incidents.	No deviations noted.
10. Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inquired of the Program Manager and determined information security incidents were documented per the organization's Incident Response Policy. Information from these events could be used to prevent future incidents and as examples for information security training.	No deviations noted.
	Inspected the organization's incident response policies and determined it documented the process for reporting, responding to, and monitoring information security incidents.	No deviations noted.
	Inspected relevant internal documentation and determined information security trainings were implemented. Inspected relevant documentation to determine that incidents were analysed to prevent future incidents	No deviations noted.

CO5 - Incident Management

Controls provide reasonable assurance that network and production system incidents are identified, recorded, tracked, and resolved in a complete and timely manner.

Control Description	Tests Performed by EY	Results
11. The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Inquired of the Program Manager and determined the organization had an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No deviations noted.
	Inspected the organization's incident response policy and determined policies and procedures were in place which outline a quick, effective, and orderly response to information security incidents. In addition, classification, prioritization, and escalation of security incidents per criticality are also identified and mechanisms are defined to measure and monitor the type and scope of security incidents.	No deviations noted.
	Inspected internal documentation and determined the organization maintained and periodically updated the incident response policy.	No deviations noted.

CO6 - Availability

Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.

Control Description	Tests Performed by EY	Results
1. The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inquired of the Program Manager and determined the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	No deviations noted.
	Inspected a sample of datastore configurations for a Google Cloud Platform product and determined the product was configured to replicate to support service redundancy, and availability.	No deviations noted.
	Inspected the Google Cloud Platform product's monitoring dashboard and determined resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy.	No deviations noted.
	Inspected the Google Cloud Platform product's monitoring data and determined resources were distributed across distinct, geographically dispersed processing facilities to support service availability.	No deviations noted.
2. The organization makes procedures related to the management of information processing resources available. Procedures include guidance on requesting,	Inquired of the Program Manager and determined the organization made available, procedures related to the management of information processing resources. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	No deviations noted.

CO6 - Availability

Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.

Control Description	Tests Performed by EY	Results
monitoring and maintaining resources, and guidance around evaluating capacity demand.	Inspected the organization's resource management documentation and determined an overview to monitor, maintain and evaluate storage and processing capacity demand had been provided.	No deviations noted.
	Inspected a sample monitoring dashboard and determined they are used to monitor and manage capacity of its information processing resources. Inspected a sample of automated notifications related to critical resource capacity utilization and determined alerts were appropriately set.	No deviations noted.
3. Internal system clocks are synchronized to atomic clocks and GPS.	Inquired of the Program Manager and determined that internal system clocks were synchronized to atomic clocks and GPS.	No deviations noted.
	Inspected internal documentation and determined Google established time synchronization service to a single reference time source.	No deviations noted.
	Inspected the relevant configurations and determined that internal system clocks were synchronized to atomic clocks and GPS.	No deviations noted.
	Inspected evidence showing the synchronization of internal system clocks to atomic clocks and GPS.	No deviations noted.
4. The organization maintains business continuity plans to	Inquired of the Program Manager and determined the organization maintains business continuity plans to define how personnel should respond to disruptions.	No deviations noted.

CO6 - Availability

Controls provide reasonable assurance that data is replicated across geographically dispersed locations, such that redundancy exists and that measures have been taken to reduce the risk of interruption to business operations.

Control Description	Tests Performed by EY	Results
define how personnel should respond to disruptions.	Inspected internal websites and determined that business continuity plans were maintained and made available to corresponding data center teams for organization-owned and third-party data centers.	No deviations noted.
	Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample of the Organization-owned data centers and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.
	Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample third-party data center and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.