System and Organization Controls (SOC) 2+ Cloud Security Alliance Cloud Control Matrix v4.0 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 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 accompanying description titled "Description of the Google Cloud Platform System" (Description) of Google LLC ("Google" or "Service Organization") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Google Cloud Platform System (System) that may be useful when assessing the risks arising from interactions with the System, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA Trust Services Criteria and the criteria set forth in the Cloud Security Alliance ("CSA") Cloud Controls Matrix ("CCM") Version 4.0 control specifications ("CCM criteria").

Complementary user entity controls: The Description also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with Google's controls to achieve the service commitments and system requirements. The Description presents Google's controls and the complementary user entity controls assumed in the design of Google's controls.

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

(a) The Description presents the System that was designed and implemented throughout the period 1 May 2023 to 30 April 2024 in accordance with the Description Criteria
(b) The controls stated in the Description were suitably designed throughout the period 1 May 2023 to 30 April 2024 to provide reasonable assurance that Google's service commitments and system requirements would be achieved based on the applicable trust services criteria and CCM criteria, if its controls operated effectively throughout the period 1 May 2023 to 30 April 2024 and if user entities applied the complementary user entity controls assumed in the design of Google's controls throughout the period.
(c) The Google controls stated in the Description operated effectively throughout the period 1 May 2023 to 30 April 2024 to provide reasonable assurance that Google's service commitments and system requirements were achieved based on the applicable trust services criteria and CCM criteria, if the complementary user entity controls assumed in the design of Google's controls operated effectively throughout that period.

Google LLC
31 August 2024

SECTION II - Independent Service Auditor's Report

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

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

Building a better working world

Independent Service Auditor's Report

To the Management of Google LLC:

Scope

We have examined Google LLC's (referred to hereafter as "Google" or "the Company") accompanying description titled "Description of the Google Cloud Platform System" of its Google Cloud Platform system for the Infrastructure as a Service (IaaS), 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 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period 1 May 2023 to 30 April 2024 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA Trust Services Criteria and the criteria set forth in the Cloud Security Alliance ("CSA") Cloud Controls Matrix ("CCM") Version 4.0 control specifications ("CCM criteria").

Complementary user entity controls: The Description indicates that Google's controls can provide reasonable assurance that certain service commitments and system requirements 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 include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information in the accompanying "SECTION V - Other Information Provided by Google LLC" is presented by management of Google to provide additional information and is not part of Google's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

Google's responsibilities

Google is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that its service commitments and system requirements were achieved. Google has provided the accompanying assertion titled, "Google's Management Assertion" (Assertion), about the presentation of the Description based on the Description Criteria and suitability of the design and

operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria and CCM criteria. Google is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the trust services and CCM criteria categories addressed by the engagement and stating the applicable trust services criteria, CCM criteria, and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls stated therein to achieve the service organization's service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and CCM criteria throughout the period 1 May 2023 to 30 April 2024. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria and CCM criteria
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria

- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and CCM criteria
- Testing the operating effectiveness of those controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and CCM criteria
- Evaluating the overall presentation of the Description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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

Inherent limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria and CCM criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria and CCM criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

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

Building a better working world

Opinion

In our opinion, in all material respects:

(a) The Description presents the Google Cloud Platform System that was designed and implemented throughout the period 1 May 2023 to 30 April 2024 in accordance with the Description Criteria
(b) The controls stated in the Description were suitably designed throughout the period 1 May 2023 to 30 April 2024 to provide reasonable assurance that Google's service commitments and system requirements would be achieved based on the applicable trust services criteria and CCM criteria, if its controls operated effectively throughout that period and if user entities applied the complementary controls assumed in the design of Google's controls throughout that period.
(c) The controls stated in the Description operated effectively throughout the period 1 May 2023 to 30 April 2024 to provide reasonable assurance that Google's service commitments and system requirements were achieved based on the applicable trust services criteria and CCM criteria, if the complementary user entity controls assumed in the design of Google's controls operated effectively throughout that period.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Google, user entities of the Google Cloud Platform System during some or all of the period 1 May 2023 to 30 April 2024 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the services provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The applicable CCM criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

Building a better working world

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

31 August 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 (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Madrid (1), Spain
- Madrid (2), Spain
- Madrid (3), Spain
- Middenmeer, Noord-Holland, The Netherlands
- Milan (1), Italy
- Milan (2), Italy
- Milan (3), Italy+
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Tel Aviv (3), Israel
- Turin (1), Italy
- Turin (2), Italy
- Turin (3), Italy
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland
- Zurich (1), Switzerland
- Zurich (2), Switzerland
- Zurich (3), Switzerland*

Asia Pacific

- Changhua, Taiwan
- Delhi (1), India
- Delhi (2), India
- Delhi (3), India*
- 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. Relevant Aspects of Internal Control

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

- **Control Environment:** Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure
- **Information and Communication:** Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control its operations
- **Risk Assessment:** The entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed across the internal and external control environment, including third-party risk

- **Monitoring Activities:** The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant
- **Control Activities:** Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's control objectives are effectively carried out

This section briefly describes the four (4) essential characteristics and other interrelated components of internal controls that support the achievement of the applicable trust services principles and criteria for security, availability, confidentiality, and privacy as it pertains to the Google Cloud Platform products that may be relevant to customers into four broad areas:

- Policies (Control Environment and Risk Assessment) – The entity has defined and documented its policies relevant to the particular principle
- Communications (Information and Communication) – The entity has communicated its defined policies to responsible parties and authorized users of the system
- Procedures (Control Activities) – The entity placed in operation procedures to achieve objectives in accordance with its defined policies
- Monitoring (Monitoring Activities) – The entity monitors the system and takes action to maintain compliance with its defined policies

With respect to internal controls and relevant customers, Google defines Customers as enterprise users that have entered into an agreement, under which Google has agreed to provide Google Cloud Platform services as a data processor.

C. Policies

Internal Control Environment

Google has designed its internal control environment with the objective of providing reasonable, but not absolute, assurance as to the security, availability, confidentiality, and privacy of financial and user information, as well as the protection of assets from unauthorized use or disposition. Management has established and maintains an internal control structure that monitors compliance with established policies and procedures.

Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, confidentiality, and privacy controls.

To maintain internal compliance, Google has established a disciplinary process for non-compliance with the Code of Conduct, security and privacy policies, and other personnel requirements which could include dismissal, lawsuits, and/or criminal prosecution.

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

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Google Cloud Platform System. Commitments to customers are communicated via Terms of Service, Google Cloud Platform System Service Level Agreements, and/or Data Processing

Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

System Requirements

Google has established internal policies and processes to support the delivery of Google Cloud Platform System products to customers. These internal policies are developed in consideration of legal and regulatory obligations, to define Google's organizational approach and system requirements.

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

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

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

Internal Functions and Policies

Google has established company structures and reporting lines and has helped ensure sufficient authorities are available to support compliance activities with regulatory, legal, contractual, and

privacy requirements. Formal organizational structures exist and are available to Google personnel on the Company's intranet. The intranet provides drill-down functionality for identifying personnel in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Google has also developed the Data Security Policy, Data Classification Guidelines and Security Labels for Google Information and Privacy policies to establish procedures for information labeling and handling in accordance with the Google guidelines. Additionally, Google maintains policies that define the requirements for the use of cryptography and policies for securing mobile devices to help ensure company and customer data are protected. Security and Privacy policies are reviewed annually, and other materials derived from policies, like guidelines, frequently asked questions (FAQs), and other related documents are reviewed and updated as needed.

D. Communications

Information and Communication

To help align its business strategies and goals with operating performance and controls, Google has implemented various methods of communication to ensure that all interested parties and personnel understand their roles and responsibilities and to ensure that significant events are communicated in a timely manner. These methods include:

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

Google has communicated to employees and extended workforce (i.e., temporary workers, vendors, and contractors) instructions and mechanisms for reporting potential security and privacy concerns or incidents. Google has also implemented various methods of communication to help ensure that user entities understand Google's commitments to security, availability, confidentiality, and privacy for Google Cloud Platform; and to help ensure that significant events are communicated to user entities in a timely manner. The primary conduit for communication is the Google website, which is made available to all user entities. This includes blog postings on

the Official Google Blog and various product specific blogs support forums, and release notes. Google provides 24 x 7 assistance, including online and phone support to address customers' concerns. Customer service and/or technical support representatives are also an important communication channel, as they maintain records of problems reported by the user entity. Customer service representatives also assist in communicating information regarding new issues and/or developments, changes in services, and other information. Additionally, Google maintains an established Board of Directors that operates independently from management. The Board exercises oversight over management decisions.

As a data processor, Google limits processing to what is specified in the contracts with the controller or as otherwise required under applicable data protection laws. Customer data is processed in accordance with the Data Processing Addendum and is externally published (see https://cloud.google.com/terms/data-processing-terms and https://workspace.google.com/terms/dpa_terms.html). As data controllers, customers are responsible for communicating choices available to users regarding collection, use, retention, disclosure and disposal of personal information. Google does provide customers with mechanisms to access, modify, delete, and export customer data.

E. Procedures

Hiring Practices

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

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

Risk Management

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

At a corporate level, there are multiple functional areas, Legal, Information Security, Internal Audit, 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 Google Cloud Platform. Google has developed vulnerability management guidelines and regularly analyzes the vulnerabilities associated with the system environment. Google takes into consideration various threat sources such as insider attacks, external attacks, errors and omissions, and third-party related issues such as inadvertent disclosure of Google confidential information (for example, payroll data) by a third party.

Factors including threat-source motivation and capability, the nature of the vulnerability, and existence and effectiveness of current controls are considered in determining the probability that a potential vulnerability may be exposed. The likelihood that a potential vulnerability could be exposed by a given threat-source is designated by Google as high, medium, or low.

Google then determines the potential adverse impact resulting from a successful exploitation of vulnerabilities. The highest priority is given to any potential compromise of user data.

The level of risk and remediation priority for a particular threat/vulnerability pair is expressed as a function of:

- The likelihood of a given threat-source's attempt to exploit a given vulnerability
- The impact should a threat-source successfully expose the vulnerability
- The effectiveness of existing security and privacy controls for mitigating risk

Google performs formal risk assessments for each of their in-scope product areas at least annually and determines the likelihood and impact of identified risks, using qualitative and quantitative methods. The likelihood and impact associated with each risk is determined independently, considering each risk category. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management. Management also proactively identifies emerging risks for product areas to include within their respective risk assessments.

Google has an established Internal Audit function and compliance specialists responsible for evaluating the effectiveness of controls in addressing a given risk, including, among other controls, identity management, source code management, and authentication infrastructure controls against requirements. They perform risk-based assessments and issue audit reports regarding their analysis. Remediation of security and privacy deficiencies are tracked through internal tools and remediation plans.

Third-Party Risk Management

Google may utilize third-party vendors to support Google Cloud Platform. Prior to onboarding, Google completes the nondisclosure agreement (NDA) then performs the vendor security assessments (VSA) on all vendors with whom Google shares confidential or sensitive information, including user data. A VSA is an important health check of a vendor's operational security posture. It assesses if a vendor adheres to generally accepted security and data protection best practices. The outcome of a VSA is a risk assessment and an approval that determines if a vendor should or can be used. At a high level, each of these assessments involves:

- An initial risk assessment to determine if a VSA is required or not such as instances where vendors handle, collect, or access any User Data, or Business Data that is classified as Need-to-Know
- A risk-based review of the policies, processes, and controls the vendor has in place compared to generally accepted security best practices using questionnaire-based information gathering
- A tailored risk assessment for Mergers and Acquisitions due diligence or third-party risk management in partnerships, joint ventures, and other complex relationships
- Reviewing and citing independent verification of the security state of systems relevant to Google's use of the vendor

A subset of vendors are considered to be subprocessors based on the data sharing relationship between the vendor and Google. Google utilizes subprocessors to support Google Cloud Platform, and has established expectations for subprocessors related primarily to security and privacy. The meeting of these expectations are subject to periodic review by Google. However, subprocessors do not manage or perform any Google Cloud Platform controls tested herein.

Google maintains a Subprocessor Audit Program that is tasked with the periodic information security and privacy assessment of subprocessors using ISO 27001 as the baseline. Google evaluates conformance to these expectations through inspection of third-party ISO certifications, SOC 2 reports, or onsite/virtual inspections. In the case that Google identifies any deviations in the performance of subprocessor controls, findings are evaluated by Google and discussed with the subprocessors upon completion of the audit. When applicable, remediation plans are put in place to timely resolve issues.

Google has also implemented a Subprocessor Data Processing Agreement (SDPA) to contract with subprocessors. The SDPA defines the security and privacy obligations which the subprocessor must meet to satisfy Google's obligations regarding customer data, prior to Google granting such access. Per the Data Processing Addendum, Google notifies the customer prior to onboarding a new subprocessor. Information about the subprocessor including function and location is externally published (see https://cloud.google.com/terms/subprocessors and https://workspace.google.com/intl/en/terms/subprocessors.html).

Enterprise agreements are signed between Google and the Multi-Cloud Service Third-Party Providers, which outline the expectations for subprocessors related primarily to security and privacy through Service Terms. Information about Multi-Cloud Service Third-Party Providers and their locations is published (see https://cloud.google.com/terms/mcs-providers).

Data Confidentiality and Privacy

Google has established training programs for privacy and information security to support data confidentiality and privacy. Relevant Google personnel are required to complete these training programs within 90 days of joining the organization and annually thereafter. All new product and product-feature launches that include collection, processing, or sharing of user data are required to go through an internal security and privacy design review process. These reviews are performed by the security, legal, and privacy teams. Databases and websites exist to track and monitor progress of Google Cloud Platform project developments. In addition to the preventative controls, Google has also established detective measures to investigate and determine the validity of security threats. In the case of an incident there are incident response processes to report and handle events related to topics such as security and confidentiality. Google establishes

confidential agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchange with external parties.

For government agency data requests, Google has mechanisms in place to record and track transfers and disclosures of users data to third parties. Customers are notified of third party data requests in accordance with any procedure and time period agreed in the contract, unless such disclosure is prohibited by law. As a data processor, Google limits disclosures of customer data to disclosures that are legally required or authorized by the data controller.

For Google-Managed Multi-Cloud Services, responsibilities of Multi-Cloud Service Third-Party Providers are defined in the Enterprise Agreements signed between them and Google. MCS Third-Party Providers are obligated to notify Google of any law enforcement data requests, which subsequently might impact Google customers.

Information Security Program

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

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

Google has security policies that have been reviewed and approved by management and are published and communicated to employees and extended workforce with access to the Google intranet. Google's security policies describe security objectives, provide a security framework, and emphasize the importance of security to Google's business.

Information Privacy Program

Google's Information Privacy program is designed to safeguard information assets against unauthorized use, access, disclosure, modification, damage, or loss, as well as the privacy of customer data. The program includes, but is not limited to, developing and managing privacy policies, developing privacy requirements for products and services including reviewing data usage to ensure processing of customer data is in accordance with the applicable data protection agreements entered into between Google and customers based on applicable data protection laws and regulations, and developing mechanisms to react to privacy incidents and events that could affect Google's information assets and customer data. Google has dedicated privacy teams responsible for educating Google personnel about privacy, assisting product teams with privacy design, and overseeing privacy practices at the company. Google has privacy policies that have been reviewed and approved by management and are published and communicated to employees and vendors with access to the Google environment. Google's privacy policies

describe privacy objectives, provide a privacy framework and required practices, and emphasize the importance of privacy to Google's business.

Google's role as a data processor and the scope of the processing are defined in the applicable Data Processing Addendum (see https://cloud.google.com/terms/data-processing-terms and https://workspace.google.com/terms/dpa_terms.html)

Network Architecture and Management

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

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

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

Google has a firewall configuration policy that defines acceptable ports that may be used on a Google firewall. Only authorized services and protocols that meet Google's requirements are permitted access to the network. The firewalls are designed to automatically deny all unauthorized packets not configured as acceptable. Administrative access to the firewalls is limited to authorized administrative personnel using the Secure Shell (SSH) protocol and two-factor authentication. Changes to network configurations are peer reviewed and approved prior to deployment. Google has implemented automated controls on network devices to identify distributed denial of service (DDOS) attacks. Google has established incident response processes to report and handle such events (see the Incident Management section).

Authentication, Authorization, and Administration

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

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

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

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

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

Password Guidelines

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

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

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

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

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

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

Physical Access — Data Center Physical Security

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

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

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

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

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

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

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

Change Management

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

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

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

The change process starts with a developer checking out a copy of source code files from the source code management system to modify them. Once development is complete, the developer initiates applicable testing and code reviews. Once the change has received the appropriate code review, the change can be submitted making it the new head version. Google requires that

production code reviewers be independent of the developer assigned to the change and follows Google coding standards, in accordance with their policy. Production code reviews are systematically enforced.

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

Vulnerability Management

The goal of Google's Vulnerability Management program is to investigate and respond to all relevant security vulnerabilities. The Vulnerability Management Guidelines describe how vulnerabilities are detected, classified, and remediated at Google. As part of this program, the security operations team conducts network vulnerability scans to detect vulnerabilities in software, systems, and network devices. These scans are conducted on an ongoing basis, to identify and remediate potential vulnerabilities.

Also, external third-party penetration tests are performed on an annual basis for a predetermined subset of the services included in the Google Cloud Platform System, and corrective actions are taken as necessary. The subset of services included in any given year are determined by the Google Security and the Office of Compliance & Integrity teams and is based on their understanding of the organization's current risk environment, as well as the organization's current regulatory and compliance requirements.

Incident Management

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

Incident Alert and Recording

Automated signals generate alerts whenever an anomaly occurs. Production monitoring tools, in response to an anomaly, automatically generate alerts to relevant teams. An anomaly may also be manually documented by Google personnel when an issue is identified in response to a

customer service request or reported through externally available channels. Production systems are configured to send system events to monitoring and alerting tools. Google personnel use these tools to respond to potential incidents, including security and privacy incidents.

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

Incident Escalation

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

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

Incident Resolution

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

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

The incident ticket is closed upon resolution of the incident. Google also has an established post mortem process for performing technical analysis of incidents after the fact to identify root cause issues, document lessons learned, and implement fixes to strengthen and improve security controls, and to prevent future incidents. Processes for notifying customers of data security and privacy incidents that affect their accounts in accordance with disclosure laws or contractual agreements are established and implemented.

Data Retention and Deletion

Google has procedures in place to dispose of confidential and need-to-know information according to the Google data retention and deletion policy. Additionally, Google maintains defined terms regarding the return, transfer, and disposal of user data and makes these terms available to customers.

Storage Media Security

Integrity checks are in place at the application level and file system level to ensure data integrity. At the application level, checksum comparison is performed to protect against upload corruptions. File system consistency checks are also deployed at the storage layer using user-level programs which verify the integrity of the data. At the machine level, an integrity check system is used to synchronize system files on the root partition of production machines with a standard base image.

Google utilizes barcodes and asset tags to track the status and location of data center equipment from acquisition to installation, retirement, and destruction. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Google hard drives leverage technologies such as Full Disk Encryption (FDE) and drive locking, to protect data at rest. Personally Identifiable Information (PII) on removable media leaving Google facilities is approved and encrypted.

When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multi-stage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

Redundant Architecture

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

The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Google uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

Disaster Recovery

To minimize service interruption due to hardware failure, natural disaster, or other catastrophes, Google designs its infrastructure and services to be resilient to failures of software, hardware, or facilities. Redundant architecture and resources are distributed across at least two (2)

geographically dispersed data centers to support the availability of services. Network connections between the data centers help ensure swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage and system administration.

Google's Disaster Recovery program enables continuous and automated disaster readiness, response, and recovery of Google's business, systems, and data. Google conducts disaster recovery testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, failover scenarios, operational transition, and other emergency responses. Teams that participate in the disaster recovery exercise develop testing plans and post-mortems which document the results and lessons learned from the tests.

Additionally, business continuity plans defining how personnel should respond to disruptions are made available internally and maintained. Disaster resiliency testing which covers reliability, survivability, and recovery is also conducted on an ongoing basis, and at least annually.

F. Monitoring

Functional areas across the organization are accountable for designing, implementing and operating controls to reduce risk across the organization, and engage with management for assessing controls. Management performs periodic assessments of the control environment for specific areas, such as identity management, source code management and authentication infrastructure controls. Google plans and coordinates system security and privacy-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users. Independent Internal Audit teams also perform regular audits over these areas of the control environment and the reports associated with the audits are made available to the audit committee and stakeholders. In addition, monitoring activities have been described below to communicate how monitoring is performed for Google Cloud Platform.

Security Monitoring

Google has implemented monitoring tools to detect and report security events. Antivirus, phishing detection, and antimalware/antispam tools are also in place to protect Google's information assets. Google also maintains security event logs for privileged access, access to user data, authorized access attempts, and unauthorized access attempts. Logical access to security event logs is restricted to authorized personnel. Security event logs are monitored continuously using a Google proprietary Security Information and Event Management (SIEM) system to detect intrusion attempts and other security related events. The SIEM system is supplemented with codified logic which creates the "hunts" that trigger automated alerts to security personnel. The security alerts are generated for further investigation (manual and automated hunts) based on predefined thresholds. When a vulnerability has been identified, the Security team determines the appropriate response and tracks the issue through resolution. The owners of the affected component(s) determine the appropriate response, based on the severity and defined response criteria of the vulnerability.

Availability Monitoring

Resource management procedures are also established to monitor, maintain, and evaluate capacity demand. Google uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource

availability across their data centers and to validate that data has been replicated to more than one location.

Confidentiality Monitoring

Google has established incident response processes to report and handle events related to confidentiality as described under Incident Management above.

Privacy Monitoring

As described above, Google restricts and monitors access to customer data to only those with a valid business purpose, and further restricts the processing of customer data to authorized individuals. Google has an incident monitoring and response program designed to alert and take action if unauthorized access is discovered. New products and services are reviewed prior to launch to ensure customer data use is in accordance with the Data Processing Addendum.

G. 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 applicable trust services criteria 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:

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. SEF-02: Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	Customers are responsible for assigning responsibilities for the operation and monitoring of the Google Cloud Platform System.
	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.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Customers are responsible for providing the appropriate training to end-users on proper use of the Google Cloud Platform System consistent with the Acceptable Use Policies and Terms of Service. Acceptable Use Policies available at (or such URL as Google may provide): • Google Cloud Platform: https://cloud.google.com/terms/aup • Chronicle (Security Product) and Threat Intelligence for Chronicle: https://chronicle.security/legal/service-terms/
	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 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.
	Customers are responsible for training users on the use and disclosure of passwords used to authenticate to the Google Cloud Platform System.
Common Criteria 1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. Common Criteria 5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. AIS-04: Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Cloud Platform System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
CCC-01: Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	
Common Criteria 2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. Common Criteria 2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. DCS-06: Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured 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.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control. Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. BCR-07: Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Customers should contact Google if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account, compromise of data, and security events.
Common Criteria 4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Common Criteria 5.3: The entity deploys control activities through policies that establish what is	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.

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

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

Trust Services Criteria	Complementary User Entity Controls (CUECs)
and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. Privacy Criteria 5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information	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.
	Customers are responsible for enabling and enforcing the use of two-step verification on privileged administrator accounts.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. IAM-03: Manage, store, and review the information of system identities, and level of access. IAM-05: Employ the least privilege principle when implementing information system access. IAM-06: Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	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 configuring Google Cloud Marketplace permissions in Google Cloud Platform consistent with customer's internal policies (Google Cloud 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 ensuring that user data is exported and deleted from the Google Cloud Platform System before or within a reasonable amount of time after termination.
Common Criteria 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. Common Criteria 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. IAM-05: Employ the least privilege principle when implementing information system access.	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.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. susceptibilities to newly discovered vulnerabilities. BCR-03: Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Customers are responsible for configuring the Google Cloud Platform System mobile device options consistent with customer policies and procedures. Customers are responsible for configuring data storage locations that support their business and operational resiliency requirements.
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. LOG-03: Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to	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.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
responsible stakeholders based on such events and corresponding metrics.	
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Privacy Criteria 7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy. IVS-02: Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	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 establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Cloud Platform System.
Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. AIS-04: Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization. CCC-01: Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to	Customers are responsible for the deployment, configuration and modification of default security settings for cloud products including virtual machines in accordance with their information security requirements.
	Customers are responsible for 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.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Customers are responsible for managing and testing configurations that support their business and operational resiliency objectives, and for considering Google Cloud Platform architecture recommendations.
	Customers are responsible for training, testing, and deploying AI models that are used in AI-powered applications.
Common Criteria 9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. Common Criteria 9.2: The entity assesses and manages risks associated with vendors and business partners. BCR-08: Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	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.
Confidentiality Criteria 1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. Privacy Criteria 4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. Privacy Criteria 5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to	Customers are responsible for ensuring that administrators do not send unnecessary employee personal data when escalating support requests to service providers, including Google.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
meet the entity's objectives related to privacy. DSP-06: Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	

SECTION IV - Description of Criteria, Controls, Tests and Results of Tests

Description of Criteria, Controls, Tests and Results of Tests

Testing performed and results of tests of entity level controls

On the pages that follow, the applicable Trust Services Criteria and the CCM Criteria controls to meet the criteria have been specified by and are the responsibility of Google LLC and the tests performed by EY and results are the responsibility of the service auditor

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

Control criteria and related controls for systems and applications

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

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

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
1. The organization has a published policy about retention and deletion of user data.	CC6.1, C1.1, C1.2, P4.2, P4.3	Control not relevant to meet the CCM Criteria	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.
2. 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.	CC1.3, C1.1	Control not relevant to meet the CCM Criteria	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
3. Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	CC5.2, CC6.2, CC6.3, CC6.6	Control not relevant to meet the CCM Criteria	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
4. The organization has implemented a formal reporting structure that is made available to personnel.	CC1.3, CC1.4	Control not relevant to meet the CCM Criteria	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the meeting minutes of a sample Board of Directors forum and determined management considered requirements such as integrity and security when defining authorities, structures, reporting lines, and responsibilities.	No deviations noted.
			Inspected procedural documents and determined management planned and prepared for succession by developing contingency plans for assignments of responsibility.	No deviations noted.
5. The organization notifies customers of updates to its confidentiality guidelines, objectives, and practices.	CC2.3, C1.1	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.
			Inspected the organization's Terms of Service and determined the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.
			Inspected GCP's customer documentation and determined that the organization provided mechanisms to notify customers of updates to its confidentiality guidelines, objectives, and practices.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
6. Descriptions of the organization's system and its boundaries are available to external parties via ongoing communications with customers or via its official blog postings.	CC2.3	Control not relevant to meet the CCM Criteria	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.
7. The organization's privacy program is periodically reviewed for appropriateness.	P8.1	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined the organization's privacy program was periodically reviewed for appropriateness.	No deviations noted.
			Inspected internal documentation and determined the organization's privacy program was periodically reviewed for appropriateness.	No deviations noted.
			Inspected the Internal Audit report and determined the organization's privacy program was periodically reviewed by Internal Audit for effectiveness.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
8. The organization has established feedback processes that give external users the ability to voice privacy concerns, which are monitored.	P8.1	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined Google had an established feedback processes that gave external users the ability to voice privacy concerns, which are monitored.	No deviations noted.
			Inspected Google's publicly available Help and Support page and determined external users had the option to voice privacy concerns to Google.	No deviations noted.
			Observed Google's internal website and determined Google had established guidelines that customer support employees used to provide feedback to external users.	No deviations noted.
			Inspected a sample of inquiries, complaints, and disputes, and determined the cases were addressed and resolutions were monitored through to resolution.	No deviations noted.
9. The organization has an incident response program for responding to privacy incidents. Privacy incidents are monitored	P6.3, P6.5	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined the organization had an incident response program in place for responding to privacy incidents. Privacy incidents were monitored and tracked in accordance with internal policy.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
and tracked in accordance with internal policy.			Inspected internal documentation and determined the organization had an incident response program in place for responding to privacy incidents.	No deviations noted.
			Inspected a sample incident and determined that the organization had tools and dashboards available and used them to monitor and track incidents in accordance with internal policy.	No deviations noted.
10. Internal Audit performs a periodic assessment of privacy controls. Results are shared as necessary and are considered for ongoing improvement of the privacy program.	P8.1	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined Internal Audit performed a periodic assessment of privacy controls. Results were shared as necessary and were considered for ongoing improvement of the privacy program.	No deviations noted.
			Inspected internal documentation and determined Internal Audit was responsible for performing a periodic assessment of Google's privacy controls.	No deviations noted.
			Inspected the Internal Audit report and determined Internal Audit performed a periodic assessment of privacy controls. Results were shared as necessary and were considered for ongoing improvement of the privacy program.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
11. Data center perimeters are defined and secured via physical barriers.	CC6.4	Control not relevant to meet the CCM Criteria	Inquired of the Data Center Security Manager and determined data center perimeters were defined and secured via physical barriers. Access to sensitive data center zones required approval from authorized personnel and was controlled via badge readers, biometric identification mechanisms, or physical locks.	No deviations noted.
			Observed a sample of data centers and determined that access to sensitive data center facilities required approval from authorized personnel, and required two-factor authentication using badge readers, biometric identification mechanisms or physical locks.	No deviations noted.
			Inspected the Data Center Physical Access Policy and determined access was provisioned on a least-privileged basis and the facilities had segregated security zones.	No deviations noted.
			Observed a sample of data centers and determined that facilities had segregated security zones.	No deviations noted.
			Observed a sample of data centers and determined that data center perimeters were defined and secured via physical barriers.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
12. All board of directors exercise independent judgment. The independent / non-employee board of directors also demonstrate independence from management in exercising oversight of the development and performance of internal control.	CC1.2, CC1.5	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined the board of directors demonstrated independence from management and had established an audit and compliance committee to exercise oversight of the development and performance of internal control.	No deviations noted.
			Inspected the Alphabet proxy statement and determined that the board of directors, including the members of the audit and compliance committee, demonstrated independence from management.	No deviations noted.
			Inspected the Alphabet proxy statement and determined the board of directors had relevant expertise and exercised oversight over controls and performance of internal control.	No deviations noted.
			Inspected the audit and compliance committee meeting minutes for a sample meeting and determined the committee met on a quarterly basis and relevant information resulting from internal and external assessments over internal control were communicated to the board of directors.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
13. The organization reviews government agency requests for user data to determine if disclosure is required; subsequent disclosure is then limited only to that which is necessary to fulfill the request.	P6.1, P6.4	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined the organization reviewed government agency requests for customer data to determine if disclosure is required; subsequent disclosure was then limited only to that which was necessary to fulfill the request. The organization recorded and tracked transfers and disclosures of user data to third parties.	No deviations noted.
			Inspected the Google Cloud Platform Terms of Service and determined the organization was required to review government agency requests for customer data to determine if disclosure was required; subsequent disclosure was then limited only to that which was necessary to fulfill the request.	No deviations noted.
			Inspected a sample of disclosure requests in the legal request management tool and determined the organization recorded and tracked transfers and disclosure of data to third parties, and the disclosures were limited to only that which was necessary to fulfill the request.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
14. The organization records requests to disclose user data. The organization's records of requests for user data include information regarding when the request was submitted, the identity of the requester, user data that was requested, any data that had been disclosed, and when disclosure had occurred.	P6.2	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined the organization reviewed government agency requests for customer data to determine if disclosure is required; subsequent disclosure was then limited only to that which was necessary to fulfill the request. The organization recorded and tracked transfers and disclosures of user data to third parties.	No deviations noted.
			Inspected the Google Cloud Platform Terms of Service and determined the organization was required to review government agency requests for customer data to determine if disclosure was required; subsequent disclosure was then limited only to that which was necessary to fulfill the request.	No deviations noted.
			Inspected a sample of disclosure requests in the legal request management tool and determined the organization recorded and tracked transfers and disclosure of data to third parties, and the disclosures were limited to only that which was necessary to fulfill the request.	No deviations noted.
15. Where the organization is a data processor, the organization limits scope	P1.1, P2.1, P3.1, P3.2,	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined the organization limited the scope of processing to what was specified in contracts with the controller.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
of processing to what is specified in contracts with the controller.	P4.1, P4.2, P7.1		Inspected externally published documentation and determined the organization provided notice to data subjects about its privacy practices with consent obtained for the use of personal information and the organization limited the scope of processing to what was specified in contracts with controller.	No deviations noted.
			Inspected internal documentation and determined the organization limited the scope of processing to what was specified in contracts with the controller.	No deviations noted.
			Observed a user upload data to Google Cloud Platform Services and determined that Google did not use the customer provided content for purposes not specified in the data processing addendum (e.g., advertising).	No deviations noted.
16. Where the organization is a data processor, the organization maintains the necessary records of processing in accordance	P6.7	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined where the organization was a data processor, the organization maintained the necessary records of processing in accordance with the contractual obligations to controllers.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
with contractual obligations to controllers.			Inspected the Cloud Data Processing Addendum and other internal documentation and determined where the organization was a data processor, the organization maintained the necessary records of processing in accordance with the contractual obligations to controllers.	No deviations noted.
17. Logical access to network devices is restricted to authorized personnel and is periodically reviewed.	CC7.1	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined that access to network devices was restricted to authorized personnel and periodically reviewed.	No deviations noted.
			Inspected the network device access management policy and determined access to network devices was restricted to authorized personnel and periodically reviewed.	No deviations noted.
			Inspected a sample user provisioned and deprovisioned access and determined that logical access was restricted to authorized personnel.	No deviations noted.
			Inspected source code and determined logical access to network devices is restricted to authorized personnel via access rules.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample of quarterly user access reviews performed for network devices and determined the review was performed timely and by appropriate personnel.	**Deviation noted.** For one (1) quarterly review of access to network devices sampled for testing, one (1) of the 12 relevant access groups was not reviewed timely.
			Management's Response: Management acknowledges that the periodic access review for network devices for one (1) selected access group was not performed in a timely manner and completed after the defined service level objective (SLO). Management reviewed the memberships to the access group and determined that there was no inappropriate access identified as result of the delayed review. 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 semi-annual user access reviews performed for network devices and determined the review was performed timely and by appropriate personnel.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
18. Wireless connections to Corp resources at organization's facilities are encrypted	CC6.1	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined wireless connections to corporate resources at the organization's facilities were encrypted.	No deviations noted.
			Inspected internal documentation and determined wireless connections to corporate resources at the organization's facilities were encrypted.	No deviations noted.
			Inspected a remote wireless connection to corporate resources and determined that remote access to the corporate network was encrypted.	No deviations noted.
19. Where "on demand request" mechanisms are implemented to restrict human access to production resources, access requests are reviewed and approved by a second individual prior to being granted and the event is logged.	CC6.2, CC6.3	Control not relevant to meet the CCM Criteria	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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
20. The organization maintains business continuity plans to define how personnel should respond to disruptions.	CC9.1, A1.2, A1.3	Control not relevant to meet the CCM Criteria	Inquired of the Program Manager and determined the organization maintains business continuity plans to define how personnel should respond to disruptions.	No deviations noted.
			Inspected internal websites and determined that business continuity plans were maintained and made available to corresponding data center teams for organization-owned and third-party data centers.	No deviations noted.
			Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample of the Organization-owned data centers and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.
			Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample third-party data center and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
21. The organization has an internal audit function and regularly engages independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	CC5.1, CC5.2	AandA-01, AandA-02, AandA-03, AandA-04, AandA-05, AandA-06, CCC-07, CEK-09, DSP-05, GRC-01, GRC-05, GRC-06, GRC-07, STA-06, STA-08, STA-11, STA-13, STA-14, TVM-06	Inquired of the Program Manager and determined the organization had an internal audit function and regularly engaged independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	No deviations noted.
			Inspected documents related to internal audit and determined the organization had an internal audit function and regularly engaged third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security.	No deviations noted.
			Inspected a list of the organization's security compliance certifications and determined the organization regularly engaged third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the meeting invites related to the organization's annual organizational risk assessment and determined the organization's operational objectives, potential impacts, and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.
22. Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	CC4.1, CC5.3	AandA-01, AIS-01, AIS-03, AIS-04, CCC-01, CEK-01, DCS-01, DCS-02, DCS-03, DCS-04, DSP-01, DSP-05, DSP-06, GRC-01, GRC-03, HRS-02, HRS-03, HRS-04, IAM-01, IAM-02, IAM-15, IPY-01, IVS-01, LOG-01, LOG-07, SEF-01, SEF-	Inquired of the Program Manager and determined security and privacy policies are reviewed at least annually, and supporting standards, guidelines, and FAQs are created and updated as needed.	No deviations noted.
			Inspected internal documentation and determined that security and privacy policies, supporting standards, guidelines and FAQS were in place.	No deviations noted.
			Inspected internal documentation and determined security and privacy policies were reviewed at least annually and authorized before they were implemented.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
		02, STA-01, STA-11, TVM-02, UEM-01, UEM-05	Inspected the most recent security and privacy policy reviews and determined policies were approved by authorized personnel or committee, reviewed at least annually, and updated as needed.	No deviations noted.
23. The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	CC2.2, CC5.3	AandA-01, AIS-01, AIS-04, BCR-03, CEK-01, DCS-03, DSP-01, DSP-05, DSP-17, GRC-01, GRC-02, GRC-04, GRC-05, HRS-02, HRS-03, HRS-04, IAM-01, IAM-02, IAM-15, IPY-01, IVS-01, LOG-01, LOG-07, SEF-01, SEF-02, STA-01, TVM-02, UEM-01, UEM-05	Inquired of the Program Manager and determined the organization had security policies addressing confidentiality, integrity, and availability that were approved by management and published on the intranet which is accessible to employees.	No deviations noted.
			Inspected internal documentation and determined security policies addressing confidentiality, integrity and availability had been approved by management.	No deviations noted.
			Inspected internal documentation and determined the organization had security policies addressing confidentiality, integrity and availability communicated and published on the intranet and accessible to employees.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
24. The organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	CC2.1, CC2.2	AandA-01, BCR-03, BCR-05, CEK-01, CEK-06, DSP-17, GRC-01, GRC-06, HRS-02, HRS-03, HRS-04, HRS-09, HRS-13, IAM-02, IAM-05, LOG-01, SEF-01, SEF-02, SEF-07, TVM-02, TVM-05, UEM-01	Inquired of the Program Manager and determined the organization established security policies and procedures, which clearly defined information security responsibilities for all employees, including the Information Security team. The organization managed operational risk by delegating decisions on risk identification and resource prioritization.	No deviations noted.
			Inspected relevant security policies and procedures and determined they defined information security responsibilities of employees and the Information Security Team.	No deviations noted.
25. The organization has an established Internal Audit function which evaluates management's compliance with security controls.	CC4.1, CC4.2, CC5.3	AandA-02, AandA-03, AandA-04, AandA-05, CEK-09, GRC-06,	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
		GRC-07, STA-06, STA-11	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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
26. The organization periodically reviews and validates the design, operation and control record of in-scope compliance controls.	CC1.5, CC4.1, CC4.2	AandA-02, AandA-03, AandA-05, STA-11	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
27. The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, CC7.2, A1.3	AandA-03, AandA-06, AIS-03, BCR-02, BCR-03, CEK-06, CEK-07, CEK-20, DCS-12, DCS-15, DSP-01, DSP-04, DSP-09, DSP-10, GRC-01, GRC-02, GRC-03, GRC-06, GRC-07, UEM-11	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the risk assessment and determined the organization conducted periodic information security risk assessments and identified, evaluated and mitigated risks to acceptable levels based on risk criteria, which are established, documented and approved by management.	No deviations noted.
			Inspected the organization's risk assessment and determined management signed off on the annual risk assessments performed.	No deviations noted.
28. The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.	CC1.1, CC1.4, CC2.2	AandA-04, AIS-03, BCR-03, CCC-07, DCS-11, DSP-08, HRS-03, HRS-07, HRS-08, HRS-09, HRS-11, HRS-13	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample email notification sent to Google personnel and determined reminders were sent to complete the privacy and information security training within a specified time.	No deviations noted.
			Inspected the completion rate for the privacy and information security training for Google personnel and determined relevant personnel completed the trainings in the last 12 months or were actively being monitored until completion of training.	No deviations noted.
			Inspected the privacy and information security training material and determined that Google has outlined the importance of information security and maintaining user, customer and employee privacy.	No deviations noted.
			Inspected the continuing education documents and determined that the entity provided training programs to help ensure skill sets and technical competencies of existing employees and contractors were developed and maintained.	No deviations noted.
			Inspected the training activity dashboard and determined that the privacy and information security training was mandatory and required to be completed annually.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
29. The approach to meeting relevant statutory, regulatory, and contractual requirements is defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	Control not relevant to meet the SOC 2 Criteria	AandA-04, AIS-03, CEK-21, DSP-10, DSP-12, DSP-16, GRC-07	Inquired of the Program Manager and determined the approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	No deviations noted.
			Inspected the relevant documents and determined the approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	No deviations noted.
			Inspected internal documentation and determined all relevant information regarding a launch is documented, kept up to date, and reviewed by appropriate product counsels.	No deviations noted.
			Inspected meeting agenda and determined privacy regulations, contractual requirements, and general privacy topics are discussed on a weekly basis.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected meeting notes and determined product teams regularly interact with the Product Counsels to review the relevant statutory, regulatory, and contractual requirements.	No deviations noted.
			Inspected a sample of product launches for GCP and determined the launches were reviewed by appropriate Product Counsels.	No deviations noted.
30. The organization has guidelines specifying the security requirements for new and existing information systems.	CC5.2, CC5.3	AandA-04, BCR-05, CCC-01, CCC-03, CCC-05, CCC-07, DSP-07, DSP-08	Inquired of the Program Manager and determined Google had an established policy specifying the security requirements for new information systems, or enhancements to existing information systems.	No deviations noted.
			Inspected internal policies and determined security requirements were specified for new information systems, or enhancements to existing information systems.	No deviations noted.
			Inspected publicly available documentation and determined Google outlined security requirements for new information systems, or enhancements to existing information systems related to its services.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
31. Action items identified from the results of internal audit control testing are assigned an owner and tracked to ensure remediation.	P8.1	AandA-06	Inquired of the Program Manager and determined action items identified from the results of internal audit control testing were assigned an owner and tracked to ensure remediation.	No deviations noted.
			Inspected the internal audit report and determined action items identified from the results of internal audit control testing were assigned an owner and tracked to ensure remediation.	No deviations noted.
			Inspected action items from prior period internal audit testing and determined they were tracked to ensure remediation.	No deviations noted.
32. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by management.	CC3.1, CC3.2, CC3.3, CC3.4	AandA-06, AIS-03, BCR-02, BCR-03, CEK-07, DCS-05, DSP-04, DSP-10, GRC-02, GRC-06, GRC-07	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
33. The organization develops and maintains a risk management	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2	AandA-06, AIS-03, BCR-02, BCR-03, CEK-07,	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
framework to manage risk to an acceptable level.		DSP-04, DSP-09, DSP-10, GRC-01, GRC-02, GRC-03, GRC-06, GRC-07	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	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.
34. The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	CC5.3, CC7.5	AIS-01, AIS-02, AIS-04, AIS-05, AIS-06, AIS-07, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, CCC-06, CCC-07, CCC-08, CCC-09, CEK-05, CEK-06, DSP-07, DSP-08, IAM-09, IAM-12, TVM-03, UEM-07	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.
35. The organization uses a version control system, to manage source code, documentation, release labeling, and other	CC6.1, CC8.1	AIS-01, AIS-02, AIS-04, AIS-05, AIS-06, AIS-07, CCC-01, CCC-02, CCC-03, CCC-04,	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
functions. Access to the system must be approved.		CCC-05, CCC-09, DSP-07, DSP-08, TVM-03	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.
36. The organization has policies and guidelines governing the secure development lifecycle.	CC8.1	AIS-01, AIS-02, AIS-04, AIS-05, AIS-06, AIS-07, CCC-01, CCC-02, CCC-03, CCC-05, CCC-07, CCC-08, CCC-09, DSP-07, DSP-08, TVM-05, UEM-03	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
37. Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	C1.1	AIS-01, AIS-02, AIS-04, AIS-05, AIS-06, AIS-07, CCC-02, CCC-07, DSP-03, DSP-05, DSP-07, DSP-08	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.
38. The organization maintains policies regarding the return, transfer, and disposal of user data and makes	P1.1, P2.1, P4.2, P4.3	AIS-01, CCC-04, IPY-02, IPY-03, IPY-04	Inquired of the Program Manager and determined the organization maintained policies regarding the return, transfer, and disposal of user data and made these policies available to customers.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
these policies available to customers.			Inspected publicly available documentation and determined the organization had policies regarding the return, transfer, and disposal of user data and made these policies available to customers.	No deviations noted.
			Inspected the organization's internal policies and determined guidelines were established to govern the retention and deletion of user data.	No deviations noted.
			Inspected a sample of deleted files and determined an automated deletion mechanism was implemented and confidential information was disposed of as per the guidelines.	No deviations noted.
39. The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege.	CC6.1	AIS-01, DCS-02, DSP-01, DSP-17, IAM-02, IAM-04, IAM-05, IAM-08, IAM-09, IAM-10, IAM-12, IAM-14, IAM-16, LOG-04, LOG-09	Inquired of the Program Manager and determined the organization had an established policy to ensure access to information resources, including data and the systems which store or process data, was authorized based on the principle of least privilege.	No deviations noted.
			Inspected internal policies and determined access to information resources, including data and the systems which store or process data, was provisioned based on the principle of least privilege.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
40. The organization has policies and guidelines in place for the exchange of information.	Control not relevant to meet the SOC 2 Criteria	AIS-01, DSP-01, DSP-10	Inquired of the Program Manager and determined the organization had policies and procedures in place for the exchange of information.	No deviations noted.
			Inspected relevant documentation and determined the organization had policies and procedures in place for the exchanges of information.	No deviations noted.
41. The organization has policies and guidelines in place which govern the use and protection of identifiable data.	Control not relevant to meet the SOC 2 Criteria	AIS-01, DSP-03, DSP-08, GRC-02	Inquired of the Program Manager and determined the organization had policies and procedures in place which govern the use and protection of personally identifiable information.	No deviations noted.
			Inspected relevant documentation and determined the organization had policies and procedures in place which govern the use and protection of personally identifiable information, as required by relevant legislation and regulation as applicable.	No deviations noted.
42. The organization's security measures, and a commitment not to degrade security are documented, and made available to customers	Control not relevant to meet the SOC 2 Criteria	AIS-01, DSP-11, IPY-04, STA-10	Inquired of the Program Manager and determined security measures, a commitment not to degrade security, and a commitment to data protection in the event of sub-processing of customer data were documented and made available to customers.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the Cloud Data Processing Addendum (Customers) available publicly and determined security measures and a commitment not to degrade security were made available to customers.	No deviations noted.
			Inspected Service Level Agreement and determined performance measures and indicators such as system uptime were documented.	No deviations noted.
			Inspected publicly available website and determined procedures had been established for Google Cloud Product service recovery and reporting of issues.	No deviations noted.
			Inspected the Google Cloud Product Terms of Service agreement and determined Google's responsibilities and commitments to customers were documented.	No deviations noted.
43. The organization has policies and guidelines that govern access to information systems.	CC5.3	AIS-01, DSP-17, IAM-01, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-09, IAM-14	Inquired of the Program Manager and determined the organization established policies and procedures that govern access to information systems.	No deviations noted.
			Inspected the relevant documentation and determined Google established policies and procedures that govern access to information systems.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
44. The organization requires external parties (Service Providers) to meet security and privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	CC9.1	AIS-01, STA-01, STA-02	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample Vendor that processes Google customer data and determined that they had signed an Information Protection Addendum (IPA) or Partner Information Protection Addendum (PIPA).	No deviations noted.
45. System changes are reviewed and approved by a separate technical resource before moving into production.	CC2.1, CC8.1	AIS-02, AIS-04, AIS-05, AIS-06, AIS-07, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, CCC-07, CEK-05, DSP-07, DSP-08, IAM-09, TVM-03, UEM-07	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
46. Changes to the organization's systems are tested before being deployed.	CC8.1	AIS-02, AIS-04, AIS-05, AIS-06, AIS-07, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, CCC-07, CEK-05, DSP-07, DSP-08, TVM-03, UEM-07	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.
47. A standard image is utilized for the installation and maintenance of each production server.	CC8.1	AIS-02, AIS-04, AIS-05, AIS-06, AIS-07, CCC-02, CCC-06, CCC-07, IVS-04	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
			Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned GCNV assets. Further determined that a standard production GCNV image was utilized for the installation and maintenance of each production server. Deployment of GCNV software in the GCNV 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 GCNV software by users.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the monitoring tool configurations and determined the tools were configured to monitor GCNV production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
			Inspected the relevant configurations and determined that the authorization tool is in place, and that GCNV logs used to monitor attestation was running as configured.	No deviations noted.
			Observed a sample inspection of successful attestation and determined that the system required authorization prior to deployment to the GCNV production.	No deviations noted.
			Observed a sample inspection of unsuccessful attestation and determined that the system prevented deployment to GCNV production without appropriate authorization.	No deviations noted.
			Inspected the relevant GCNV user groups and determined access to deploy software was restricted to authorized personnel.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
48. The organization performs privacy reviews prior to product launch.	C1.1, P3.1	AIS-02, AIS-04, AIS-05, CCC-02, CCC-07, DSP-03, DSP-05, DSP-08, DSP-09	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.
49. Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Control not relevant to meet the SOC 2 Criteria	AIS-03	Inquired of the Program Manager and determined procedures for administrative operations of the organization's cloud computing environment were documented and made available to customers.	No deviations noted.
			Inspected the Google Cloud Platform website and determined procedures for administrative operations of the organization's cloud computing environment were documented and provided to customers.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
50. Where the organization is a data processor, the organization documents their legal, regulatory, and business obligations to controllers related to the processing of the user data within written contracts.	Control not relevant to meet the SOC 2 Criteria	AIS-03	Inquired of the Program Manager and determined the organization documented their legal, regulatory, and business obligations to controllers related to the processing of the customer data within written contracts.	No deviations noted.
			Inspected the Cloud Data Processing Addendum and other public documentation and determined the organization documented their legal, regulatory, and business obligations to controllers related to the processing of the customer data within written contracts.	No deviations noted.
51. The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	CC3.2, CC3.3, CC6.8, CC7.1, CC7.2	AIS-03, AIS-06, AIS-07, SEF-01, SEF-02, SEF-06, TVM-01, TVM-03, TVM-04, TVM-05, TVM-08, TVM-09, TVM-10	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
52. The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	CC9.1, A1.2, A1.3	AIS-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-09, BCR-10	Inquired of the Program Manager and determined that the organization had implemented business continuity measures to maintain the availability of the organization's production infrastructure and services.	No deviations noted.
			Inspected internal documentation and determined that the organization defined the risks and recovery objectives to establish measures that maintain the availability of its production infrastructure and services.	No deviations noted.
			Inspected the documentation that establishes measures to maintain the availability of the organization's production infrastructure and services.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the documentation that establishes measures to maintain the availability of the organization's production infrastructure and services and determined the documentation was tested on an interval basis or upon significant organizational or environmental changes.	No deviations noted.
			Inspected a sample team guideline available and determined it included the procedures which need to be followed in an emergency or incident.	No deviations noted.
			Inspected a sample ticket and determined recovery activities were outlined.	No deviations noted.
53. The organization has established a code of conduct that is reviewed and updated as needed.	CC1.1, CC9.2, C1.1	AIS-03, CCC-05, DCS-11, HRS-07, HRS-08, HRS-09, HRS-12, IAM-10, STA-11	Inquired of the Program Manager and determined the organization established internal privacy and information security policies available in the intranet as well as code of conduct.	No deviations noted.
			Inspected applicable policies and guidelines and determined the privacy and information security as well as code of conduct were in place.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
54. Company goals and responsibilities are required to be developed and communicated by management on a periodic basis, and amended as needed. Results are evaluated and communicated to employees.	CC1.3, CC1.5, CC2.2, CC3.1	AIS-03, GRC-06	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.
55. The organization provides supplemental training and awareness programs to employees.	Control not relevant to meet the SOC 2 Criteria	AIS-03, HRS-12	Inquired of the Program Manager and determined supplemental privacy training and awareness programs were provided by the organization to its employees.	No deviations noted.
			Inspected internal documentation and determined supplemental privacy training and awareness programs were provided by the organization to its employees.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the internal privacy workshops and training courses that were available and determined supplemental privacy training and awareness programs were provided by the organization to its employees.	No deviations noted.
			Inspected sample privacy notification and determine employees were reminded to retake the annual privacy training.	No deviations noted.
56. Penetration tests are performed at least annually.	CC4.1	AIS-03, TVM-06	Inquired of the Program Manager and determined the organization performed penetration tests by qualified internal personnel or an external service provider at least annually.	No deviations noted.
			Inspected relevant documentation and determined the organization has policies and guidelines in place for penetration tests performed by qualified internal personnel or an external service provider.	No deviations noted.
			Inspected relevant documentation and determined a penetration test, which included critical infrastructure components, occurred within the past year and results were documented comprehensively.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the penetration test report and related documentation and determined that identified deficiencies were assessed, prioritized, followed up and addressed based on their criticality.	No deviations noted.
57. Integrity checks are in place at the application level to ensure data integrity.	CC6.7, CC7.1	AIS-04, AIS-05	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.
58. Integrity checks are in place at the file system level to ensure data integrity.	CC7.1	AIS-04, AIS-05	Inquired of the Program Manager and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a Software Engineer modify a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
			Observed a Software Engineer delete a sample file in the directory of a haphazardly selected production machine and determined the tool detected the deleted sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
59. The organization provides a mechanism for users to export a copy of their data in their Google Accounts to a machine-readable format, where feasible.	Control not relevant to meet the SOC 2 Criteria	AIS-04, IPY-01, IPY-02, IPY-03, IPY-04	Inquired of the Program Manager and determined the organization provided a mechanism for users to export a copy of their data in their Google Accounts in a machine-readable format, where feasible.	No deviations noted.
			Inspected public documentation, including the Cloud Data Processing Addendum, and determined the organization provided a mechanism for users to export a copy of their data in their Google Accounts in a machine-readable format.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample Google Workspace product and determined the organization provided a mechanism to export a copy of the data in a machine-readable format.	No deviations noted.
			Inspected a sample Google Cloud Platform product and determined the organization provided a mechanism to export a copy of the data in a machine-readable format.	No deviations noted.
60. Changes to network configurations are reviewed and approved prior to deployment.	CC8.1	AIS-06, AIS-07, CCC-01, CCC-02, CCC-03, CCC-05, CCC-07, CEK-05, DSP-07, IVS-04, TVM-03	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
61. The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	CC9.1, A1.2, A1.3	BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, IVS-02, SEF-03, SEF-04	Inquired of the Program Manager and determined that the organization conducted disaster resiliency testing (DiRT) which covered reliability, survivability, and recovery on an ongoing basis (and at least annually).	No deviations noted.
			Inspected a sample of the functional disaster resiliency testing documentation and determined that it was conducted on a periodic basis and testing was conducted to ensure continuous and automated disaster readiness, response, and recovery of business, systems and data.	No deviations noted.
			Inspected testing documentation and determined that product teams developed testing plans and postmortems which documented the results and lessons learned from disaster resiliency testing.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
62. The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	CC7.4, A1.1, A1.2, A1.3	BCR-01, BCR-02, BCR-03, BCR-05, BCR-08, BCR-11, DCS-15, DSP-16, DSP-19, IVS-02	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
63. The organization has geographically dispersed personnel responsible for managing security incidents.	Control not relevant to meet the SOC 2 Criteria	BCR-02, BCR-03	Inquired of the Program Manager and determined the organization has geographically dispersed personnel responsible for managing security incidents.	No deviations noted.
			Inspected the organization's security and privacy incident management team information and determined there are relevant personnel that are geographically dispersed to support the organization's security posture in the event of a crisis or disaster.	No deviations noted.
64. Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).	CC6.2, A1.1, A1.2	BCR-02, BCR-03, BCR-11, DCS-12, DCS-13, DCS-14, DCS-15	Inquired of the Data Center Operations Manager and determined redundant power was utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power sources.	No deviations noted.
			Observed a sample of data centers and determined that network rooms were connected to an UPS system and emergency generator power was available for at least 24 hours in the event of a loss of power.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
65. The descriptions of the organization's systems (including their scope and boundaries) are made available to internal teams.	CC2.2	BCR-03, BCR-05	Inquired of the Program Manager and determined that descriptions of the organization's systems, including their scope and boundaries, were made available to internal teams.	No deviations noted.
			Inspected the internal website for all internal products and determined 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
66. The organization has established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.	CC3.2	BCR-03, BCR-05, CCC-07, DSP-17, SEF-01, SEF-02, UEM-11	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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
67. Teams within the organization document standard operating procedures and make them available to authorized personnel	CC2.1	BCR-03, BCR-05, DCS-11, DSP-05, IPY-01	Inquired of the Program Manager and determined that teams within the organization document standard operating procedures and make them available to authorized personnel.	No deviations noted.
			Inspected internal team handbooks for a sample Google Cloud Platform product team and determined that documented standard operating procedures were in place and available to authorized personnel.	No deviations noted.
68. Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.	A1.2	BCR-03, BCR-11, DCS-12, DCS-13, DCS-14, DCS-15	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a sample of data centers and determined that temperature and humidity of data halls were within the configured thresholds.	No deviations noted.
69. Power management and distribution systems are utilized to protect critical data center equipment from disruption or damage.	Control not relevant to meet the SOC 2 Criteria	BCR-03, BCR-11, DCS-13, DCS-14, DCS-15	Inquired of the Data Center Operations Manager and determined redundant power was utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power sources.	No deviations noted.
			Observed a sample of data centers and determined that network rooms were connected to an UPS system and emergency generator power was available for at least 24 hours in the event of a loss of power.	No deviations noted.
			Observed a sample of data centers and determined that data centers were equipped with redundant network connections via different physical connections.	No deviations noted.
			Inspected maintenance records for in-scope data centers and observed that equipment was continuously monitored and periodically tested.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
70. The organization makes procedures related to the management of information processing resources available. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	CC7.1, CC7.2, CC7.3, CC7.4, CC7.5	BCR-03, BCR-11, IVS-02	Inquired of the Program Manager and determined the organization made available, procedures related to the management of information processing resources. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	No deviations noted.
			Inspected the organization's resource management documentation and determined an overview to monitor, maintain and evaluate storage and processing capacity demand had been provided.	No deviations noted.
			Inspected a sample monitoring dashboard and determined they are used to monitor and manage capacity of its information processing resources. Inspected a sample of automated notifications related to critical resource capacity utilization and determined alerts were appropriately set.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
71. The organization has a dedicated team responsible for managing security and privacy incidents.	CC7.2, CC7.3, CC7.4, CC7.5, A1.3, P6.3	BCR-07, IAM-12, IVS-02, LOG-03, LOG-04, LOG-05, LOG-10, LOG-13, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, SEF-06, SEF-07	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample of incident tickets and determined the incident response team quantified and monitored incidents.	No deviations noted.
72. The organization has established policies and guidelines to govern data classification, labeling and security.	CC6.1, C1.1, P4.1	BCR-08, CEK-04, DCS-05, DSP-01, DSP-03, DSP-04, DSP-06, DSP-15, DSP-16, DSP-17	Inquired of the Program Manager and determined the organization has established policies and guidelines to govern data classification, labeling and security.	No deviations noted.
			Inspected relevant documentation and determined Google established policies and guidelines to govern data classification, labeling and security.	No deviations noted.
73. The organization has established guidelines for governing the installation of software on organization-owned assets.	CC6.7, CC8.1	CCC-01, CCC-03, CCC-04, CCC-05, CCC-07, UEM-02	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
			Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.
			Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned GCNV assets. Further determined that a standard production GCNV image was utilized for the installation and maintenance of each production server. Deployment of GCNV software in the GCNV production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected Google's security policies and determined Google had implemented rules to govern the installation of GCNV software by users.	No deviations noted.
			Inspected the monitoring tool configurations and determined the tools were configured to monitor GCNV production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
			Inspected the relevant configurations and determined that the authorization tool is in place, and that GCNV logs used to monitor attestation was running as configured.	No deviations noted.
			Observed a sample inspection of successful attestation and determined that the system required authorization prior to deployment to the GCNV production.	No deviations noted.
			Observed a sample inspection of unsuccessful attestation and determined that the system prevented deployment to GCNV production without appropriate authorization.	No deviations noted.
			Inspected the relevant GCNV user groups and determined access to deploy software was restricted to authorized personnel.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
74. Development, testing and build environments are separated from the production environment through the use of logical security controls.	CC8.1	CCC-01, CCC-03, CCC-05, DSP-15, IVS-05	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
75. The organization authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items.	CC6.7	CCC-04, DCS-02, DCS-04, DCS-06, DCS-07, DCS-10	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
76. The organization has policies and guidelines that govern the acceptable use of information assets.	CC3.2, CC6.1	CCC-04, DCS-05, DSP-01, DSP-05, DSP-06, DSP-15, DSP-16, HRS-02, HRS-05, UEM-02	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.
77. The organization has established an offboarding procedure for personnel, which governs the removal of access and return of assets.	CC5.2	CCC-04, HRS-05, HRS-06, IAM-02, IAM-07, IAM-08, IAM-14, IAM-16	Inquired of the Program Manager and determined the organization had established offboarding procedures for personnel, which governed the removal of access and return of assets.	No deviations noted.
			Inspected internal guidelines and determined the organization had established offboarding procedures for personnel, which governed the removal of access and return of assets.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected internal guidelines and determined internal and external employees were informed that obligations to comply with relevant laws, regulations, and provisions regarding information security remain valid, even if the area of responsibility changes or the employment relationship is terminated.	No deviations noted.
78. The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	CC2.3	CCC-05, DSP-05, DSP-11, IPY-02, IPY-04, LOG-03, LOG-13, SEF-03, SEF-07, STA-09, STA-10	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.
79. The organization hardens virtual environments where it has a responsibility as outlined	Control not relevant to meet the SOC 2 Criteria	CCC-07, DSP-07, IVS-01, IVS-04	Inquired of Program Manager and determined Google hardens virtual environments where Google has a responsibility as outlined in the shared responsibilities.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
in the shared responsibilities.			Inspected Google's security page and determined Google hardens virtual environments where Google has a responsibility as outlined in the shared responsibilities.	No deviations noted.
			Inspected the log of the tool used to monitor the replication of the golden production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
			Inspected the configuration of the tool Google uses to manage production images and determined it was configured to enforce standard production image for installation and maintenance of Google servers.	No deviations noted.
			Observed a Software Engineer insert a test file in 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a Software Engineer modify a test file in 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 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.
			Inspected the relevant teams involved in the virtual hardening process and determined Google hardens virtual environments where Google has a responsibility as outlined in the shared responsibilities.	No deviations noted.
			Inspected a sample bug ticket and determined security vulnerabilities in the virtual environments are monitored and tracked.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inquired of Program Manager and determined Google hardens virtual environments where Google has a responsibility as outlined in the shared responsibilities.	No deviations noted.
			Inspected Google's security page and determined Google hardens virtual environments where Google has a responsibility as outlined in the shared responsibilities.	No deviations noted.
			Inspected the relevant configurations and determined that the authorization tool is in place, and that logs used to monitor attestation was running as configured.	No deviations noted.
			Observed a sample inspection of successful attestation and determined that the system required authorization prior to deployment to production.	No deviations noted.
			Observed a sample inspection of unsuccessful attestation and determined that the system prevented deployment to production without appropriate authorization.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample bug ticket and determined security vulnerabilities in the virtual environments are monitored and tracked.	No deviations noted.
80. Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.	CC6.8	CCC-07, IVS-01, IVS-04	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.
			Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
			Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
			Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the relevant user groups and determined access to handling exceptions, emergencies, enforcement of policies, and review of software to be deployed was restricted to authorized engineers.	No deviations noted.
			Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned GCNV assets. Further determined that a standard production GCNV image was utilized for the installation and maintenance of each production server. Deployment of GCNV software in the GCNV 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 GCNV software by users.	No deviations noted.
			Inspected the monitoring tool configurations and determined the tools were configured to monitor GCNV production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the relevant configurations and determined that the authorization tool is in place, and that GCNV logs used to monitor attestation was running as configured.	No deviations noted.
			Observed a sample inspection of successful attestation and determined that the system required authorization prior to deployment to the GCNV production.	No deviations noted.
			Observed a sample inspection of unsuccessful attestation and determined that the system prevented deployment to GCNV production without appropriate authorization.	No deviations noted.
			Inspected the relevant GCNV user groups and determined access to deploy software was restricted to authorized personnel.	No deviations noted.
81. The organization maintains policies that define the requirements for the use of cryptography.	CC6.7	CEK-01, CEK-02, CEK-03, CEK-04, CEK-05, CEK-06, CEK-07, CEK-08,	Inquired of the Program Manager and determined the organization established policies and procedures that govern the internal and external use of cryptographic controls.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
		CEK-09, CEK-10, CEK-11, CEK-12, CEK-13, CEK-14, CEK-15, CEK-16, CEK-17, CEK-18, CEK-19, CEK-20, CEK-21, DSP-10, DSP-17, LOG-10, LOG-11	Inspected the organisation's security policies and procedures and determined they covered governance of the internal and external use of cryptographic controls.	No deviations noted.
			Inspected a Google Cloud Platform relevant documentation and determined they covered governance of the internal and external use of cryptographic controls.	No deviations noted.
82. The organization has an established key management process in place to support the organization's use of cryptographic techniques.	CC6.1	CEK-01, CEK-02, CEK-03, CEK-04, CEK-05, CEK-06, CEK-10, CEK-11, CEK-12, CEK-13, CEK-14, CEK-15, CEK-16, CEK-17, CEK-18, CEK-19, CEK-20, CEK-21, DSP-10, IAM-10, LOG-10, LOG-11	Inquired of the Program Manager and determined Google had an established key management process in place to support the organization's internal cryptographic techniques.	No deviations noted.
			Inquired of the Program Manager and determined Google had an established key management process in place to support the organization's external use of cryptographic techniques.	No deviations noted.
			Inspected internal documentation and determined key management procedures were in place for internal cryptographic techniques.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected internal documentation and determined key management procedures were in place for external cryptographic techniques.	No deviations noted.
			Inspected the code configuration and determined that internal certificates expired after a set duration when the certificate is issued.	No deviations noted.
			Inspected the code configuration for internal certificate revocations and determined certificate revocations conformed to Google policies and procedures and changes to the list of certificate revocations were restricted with proper authorizations.	No deviations noted.
			Inspected the code configuration enforcing encryption and certificate authentication and determined internal use of cryptographic techniques conformed to Google policies and procedures.	No deviations noted.
			Inspected the code configuration enforcing encryption and certificate authentication and determined external use of cryptographic techniques conformed to Google policies and procedures.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the code configuration for external certificate revocations and determined certificate revocations used proper authorizations and changes to the list of certificate revocations were restricted.	No deviations noted.
			Observed an engineer attempt to request a certificate and determined the key management process was followed to support the organization's internal use of cryptographic techniques.	No deviations noted.
			Inspected a sample of internal certificate revocation requests and determined certificates were revoked timely.	No deviations noted.
			Observed an engineer attempt to request a certificate and determined the key management process was followed to support the organization's external use of cryptographic techniques.	No deviations noted.
			Inspected a sample of external certificate revocation requests and determined certificates were revoked timely.	No deviations noted.
83. The organization ensures that cryptographic controls are used in compliance with relevant	Control not relevant to meet the	CEK-01, CEK-03, CEK-05, CEK-06, DSP-10, DSP-17,	Inquired of the Program Manager and determined that cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
agreements, laws, and regulations.	SOC 2 Criteria	IVS-07, LOG-10, LOG-11	Inspected the applicable compliance and regulatory requirements policies and determined that cryptographic controls are required to be used in compliance with all relevant agreements, laws, and regulations.	No deviations noted.
84. The organization uses encryption protocols to secure user data in transit between users and the organization's production facilities	Control not relevant to meet the SOC 2 Criteria	CEK-01, CEK-03, DSP-10, DSP-17, IPY-03, IVS-03, IVS-07	Inquired of the Program Manager and determined the organization encrypted end user traffic while in transit.	No deviations noted.
			Inspected documentation and determined the organization encrypted end user traffic while in transit.	No deviations noted.
			Inspected the configuration and determined the organization encrypted end user traffic while in transit.	No deviations noted.
			Inspected the server scan results and determined Google used encryption mechanism to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
85. The organization uses encryption to secure user data in transit between the	CC6.7	CEK-01, CEK-03, DSP-10, DSP-17,	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
organization's production facilities.		IVS-03, IVS-06, IVS-07	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.
86. The organization has established guidelines for protecting against the risks of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems.	CC6.1, CC6.7	CEK-01, CEK-03, DSP-10, HRS-02, HRS-04	Inquired of the Program Manager and determined Google has established guidelines for protecting against the risk of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems. Google also requires two-factor authentication and valid certificates to be installed on the connecting device.	No deviations noted.
			Inspected relevant documentation and determined guidelines and policies were implemented to protect information accessed and govern the use of system encryption for communication.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected authentication settings for production and remote access and determined access to the system required two-factor authentication and valid certificates to be installed on the connecting device.	No deviations noted.
			Inspected connection settings for a user connecting to the Google network and determined that encryption mechanisms were used.	No deviations noted.
			Observed a user attempt to gain access to the environment with a device that had Google issued digital certificates installed and determined access was successful.	No deviations noted.
			Observed a user attempt to gain access to the environment with a device that did not have Google issued digital certificates installed and determined access was denied.	No deviations noted.
87. External system users are identified and authenticated via the Google Accounts or the BYOID authentication	CC6.1	CEK-01, CEK-03, DSP-10, IAM-02, IAM-06, IVS-03	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
system before access is granted.			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.
88. Only users with a valid user certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	CC6.6, CC6.7	CEK-01, CEK-03, DSP-10, IAM-10, IAM-14, IAM-16, IVS-03	Inquired of the Program Manager and determined only users with a valid certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	No deviations noted.
			Inspected relevant documentation and determined mechanisms are in place to authenticate users and restrict access to production machines without a valid digital certificate.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
89. Encryption is used to protect user authentication and administrator sessions	CC6.1, CC6.6, CC6.7	CEK-01, CEK-03, DSP-10, IAM-	Inquired of the Program Manager and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
transmitted over the Internet.		15, IVS-03, IVS-07	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the server scan results and determined the organization used encryption mechanisms to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
90. 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.	CC6.1, CC6.6	CEK-03, DSP-10, IAM-02, IAM-05, IAM-10, IAM-14, IAM-16, IVS-06	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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
91. The organization has implemented perimeter devices to protect the corporate network from external network attacks.	CC6.6	CEK-03, DSP-10, IAM-14, IAM-16, IVS-03, IVS-08, IVS-09, UEM-10	Inquired the Program Manager and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
			Inspected the policies and documents related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
			Inspected the configurations related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
92. Customer data that is uploaded or created is encrypted at rest.	CC6.1	CEK-03, DSP-17, IVS-07	Inquired of the Program Manager and determined customer data that was uploaded or created was encrypted at rest.	No deviations noted.
			Inspected the policies surrounding customer data encryption at Google and determined guidelines and policies were implemented to protect customer data.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the encryption configuration for storage devices with customer data at rest and determined that encryption was enabled to protect customer data.	No deviations noted.
			Inspected a sample of storage devices with customer data and determined they displayed an encrypted state.	No deviations noted.
			Inquired of the Program Manager and determined customer data that was uploaded or created for GCNV was encrypted at rest.	No deviations noted.
			Inspected GCNV system documentation and determined customer data at rest is encrypted.	No deviations noted.
			Inspected the encryption settings for a sample GCNV machine and determined customer data at rest was encrypted.	No deviations noted.
93. The organization tests, validates, and documents changes to its services prior to deployment to production.	Control not relevant to meet the SOC 2 Criteria	CEK-05	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
94. The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.	CC6.5, P4.3	DCS-01, DCS-04, DSP-02, DSP-16	Inquired of the Operations or Facilities Managers at each site and determined the organization sanitized storage media prior to disposal, release out of organizational control, or release for reuse.	No deviations noted.
			Inspected the data destruction and transportation policies and determined the organization had policies in place regarding the sanitization of storage media prior to disposal, release out of organizational control, or release for reuse.	No deviations noted.
			Inspected a sample destroyed equipment leaving Google's data centers and determined the equipment was subject to Google's sanitization and destruction process.	No deviations noted.
			Inspected the relevant configuration and determined USB ports were disabled at a global level for data centers.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the relevant configuration and determined alerts were configured to generate if thresholds for Google's sanitization processes were exceeded.	No deviations noted.
			Inspected a sample of alerts generated when thresholds for Google's sanitization processes were exceeded and determined the alerts were appropriately generated and resolved in a timely manner.	No deviations noted.
95. The organization has policies and guidelines for working in secure areas.	Control not relevant to meet the SOC 2 Criteria	DCS-02, DCS-03, DCS-07, DCS-09, DCS-10	Inquired of the Program Manager and determined that Google had developed policies and procedures for working in secure areas.	No deviations noted.
			Inspected the relevant documentation and determined Google had developed policies and procedures for working in secure areas.	No deviations noted.
96. Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	CC6.4	DCS-02, DCS-07, DCS-09, DCS-10	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
97. Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.	CC6.4	DCS-03, DCS-07, DCS-09	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.
			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.
98. Visitors to corporate offices must be authenticated upon arrival and remain with an escort	CC6.4	DCS-03, DCS-07, DCS-09, DCS-10	Inquired of the Security Officer and determined that visitors to corporate offices were required to authenticate upon arrival and remain with an escort for the duration of their visit.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
for the duration of their visit.			Inspected internal documentation and determined the organization maintained policies for visitor access to corporate offices.	No deviations noted.
			Performed inspections for a sample of offices and determined that the reception area was isolated from the office space.	No deviations noted.
			Observed an on-site sign in of a visitor to Google offices and determined visitors to corporate offices were required to authenticate upon arrival and remain with an escort for the duration of their visit.	No deviations noted.
99. The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.	CC6.4, CC6.7	DCS-03, DCS-07, DCS-09, DCS-10	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
100. Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	CC6.4	DCS-03, DCS-07, DCS-09, DCS-10, DCS-11, DCS-13, LOG-12	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a sample of data centers and determined that data centers were secured through the use of badge reader and biometric control systems.	No deviations noted.
			Inspected the badge reader activity logs for a sample of data centers and determined access to Google spaces was logged and monitored.	No deviations noted.
			Inspected the badge reader activity logs for a sample of data centers and determined logs were retained for at least 3 months.	No deviations noted.
101. Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.	CC6.4	DCS-03, DCS-07, DCS-09, DCS-10, DCS-11, LOG-12	Inquired of the Data Center Security Manager and determined data center perimeters were defined and secured via physical barriers. Access to sensitive data center zones required approval from authorized personnel and was controlled via badge readers, biometric identification mechanisms, or physical locks.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a sample of data centers and determined that access to sensitive data center facilities required approval from authorized personnel, and required two-factor authentication using badge readers, biometric identification mechanisms or physical locks.	**Deviation noted.** For one (1) of the 23 sites sampled for testing, one (1) visitor badge was provisioned with the incorrect access.
			Management's Response: Management acknowledges that incorrect access was provisioned to one visitor during the date of the BTN site visit and upon further investigation, it was determined that the incorrect access provisioned was due to a manual provisioning error. Upon noticing the error, the Regional Operations Security Center team (RSOC) adjusted the clearance level to be appropriate for the visitor and access was removed at the end of the visit as appropriate. In addition, the visitor is constantly escorted, and the visitor only had an elevated level of access when exiting the data center floor and movements were monitored by badge readers and CCTVs. As a result, the residual risk of the visitor impacting the security or reliability of the site is low and management is taking steps internally to reduce the likelihood of errors made during the manual provisioning process.	

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the Data Center Physical Access Policy and determined access was provisioned on a least-privileged basis and the facilities had segregated security zones.	No deviations noted.
			Observed a sample of data centers and determined that facilities had segregated security zones.	No deviations noted.
			Observed a sample of data centers and determined that data center perimeters were defined and secured via physical barriers.	No deviations noted.
102. Physical access to the Corporate Offices is secured via security personnel, badge readers, security credentials (badges) and/or video cameras.	Control not relevant to meet the SOC 2 Criteria	DCS-03, DCS-07, DCS-09, DCS-10, LOG-12	Inquired of the Security Officer and determined that physical access to the corporate offices was secured via security guards, access badges and video cameras.	No deviations noted.
			Inspected internal documentation and determined the organization maintained policies for security personnel, badge readers, and video monitoring.	No deviations noted.
			Performed inspections for a sample of offices and observed that physical access to the corporate offices was secured via security guards, access badges and video cameras.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected badge logs from a sample of office locations and determined badge records were retained and monitored by physical access control mechanisms.	No deviations noted.
			Observed the security camera live feed from a sample of offices and determined that the GSOC team monitored the feed on a 24/7 basis.	No deviations noted.
103. Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.	CC6.4	DCS-03, DCS-07, DCS-09, DCS-10, LOG-12	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
104. Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	CC6.4	DCS-03, DCS-07, DCS-09, DCS-10, LOG-12, SEF-06	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.
105. Automated mechanisms are utilized to track inventory of all production machines and	CC6.7	DCS-05, DCS-06, DCS-08, STA-07	Inquired of the Data Center Operations Manager and determined automated mechanisms were utilized to track inventory of production machines.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
inventory of all serialized server components.			Inspected the records from the inventory system for a sample of production machines selected during data center inspections and determined the selected machines existed in the inventory system.	No deviations noted.
			Observed a sample of production machines selected from the inventory system prior to the data center inspection and determined that the selected machines existed at the data centers.	No deviations noted.
			Inspected the 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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. 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.	
106. The Technical Infrastructure Product Area ultimately owns assets used for information processing (i.e. production machines).	Control not relevant to meet the SOC 2 Criteria	DCS-08, DSP-06	Inquired of the Program Manager and determined assets used for information processing (i.e. production machines) are owned by the Tech Infrastructure team and are allocated to individual teams upon request.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
Assets are allocated to individual teams upon request.			Inspected a sample of production machines and determined they were accounted for in the inventory system and owned by the Tech Infrastructure team.	No deviations noted.
107. Access to corporate network, production machines, network devices, and support tools requires a unique ID, password, and/or machine certificate.	CC6.1, CC6.2	DCS-08, DSP-10, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-10, IAM-13, IAM-14, IAM-16, IVS-06	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a user attempt to obtain access to network devices without first authenticating via user ID, password, security key, and/or certificate and determined that the user failed to obtain access.	No deviations noted.
			Observed a user attempt to access an internal support tool with 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.
108. Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.	CC6.1	DCS-08, IAM-02, IAM-03, IAM-05, IAM-14, IAM-16	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
109. The organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	CC6.1	DCS-08, IAM-02, IAM-14, IAM-15, IAM-16, UEM-01	Inquired of the Program Manager and determined Google had established password guidelines to govern the management and use of authentication mechanisms.	No deviations noted.
			Inspected relevant documentation and determined formal guidelines for passwords were established to govern the management and use of authentication mechanisms.	No deviations noted.
			Inspected the relevant configurations and determined passwords were transmitted and stored in an encrypted manner.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the password configurations propagated to servers and determined they were configured to enforce password requirements.	No deviations noted.
			Observed user attempt to login using incorrect password and determined the account was locked out after exceeding the maximum number of attempts allowed.	No deviations noted.
110. Data center physical access logs are recorded and retained in accordance with organizational or regulatory requirements.	Control not relevant to meet the SOC 2 Criteria	DCS-09, LOG-12	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a sample of data centers and determined that data centers were continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	No deviations noted.
			Observed a sample of data centers and determined that data centers were secured through the use of badge reader and biometric control systems.	No deviations noted.
			Inspected the badge reader activity logs for a sample of data centers and determined access to Google spaces was logged and monitored.	No deviations noted.
			Inspected the badge reader activity logs for a sample of data centers and determined logs were retained for at least 3 months.	No deviations noted.
111. Personnel of the organization are required to acknowledge the code of conduct.	CC1.1	DCS-11, HRS-02, HRS-03, HRS-07, HRS-	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
		08, HRS-09, HRS-12	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.
112. Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	CC5.2	DCS-13, DCS-14, DCS-15	Inquired of the Operations Manager and determined critical data center equipment supporting Google products and services were continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	No deviations noted.
			Inspected a sample of maintenance records for the UPS, generators, fire suppression systems, fire extinguishers, emergency lighting systems, and HVAC systems, and determined Google performed and recorded routine preventative and regular maintenance in accordance with organizational requirements over critical data center equipment.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
113. Data centers are equipped with fire detection alarms and protection equipment.	A1.2	DCS-15	Inquired of the Data Center Operations Facilities Manager and determined data centers were equipped with fire detection alarms and protection equipment.	No deviations noted.
			Observed a sample of data centers and determined that they were equipped with fire detection alarms and protection equipment.	No deviations noted.
			Observed a sample of data centers and determined that potential environmental threats to the data centers were anticipated and countermeasures were established based on the nature and geographical location of the data centers.	No deviations noted.
114. Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	CC7.2, CC7.3, CC7.4, C1.1	DSP-03, IAM-09, IAM-10, IAM-12, IVS-03, IVS-05, IVS-08, IVS-09, LOG-01, LOG-02, LOG-03, LOG-05, LOG-07, LOG-08, LOG-10, LOG-11, LOG-13, SEF-01, SEF-	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
		05, SEF-06, SEF-07	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.
			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.
115. Changes to customer facing services that may affect confidentiality, processing integrity and / or availability are communicated to relevant personnel and impacted customers.	CC2.2, CC2.3	DSP-05	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.
116. The organization has information security and data access policies and controls in place to prevent unauthorized access, alteration, disclosure, or destruction of important records.	Control not relevant to meet the SOC 2 Criteria	DSP-05, DSP-17	Inquired of the Program Manager and determined information security and data access policies and controls were in place to prevent unauthorized access, alteration, disclosure, or destruction of important records.	No deviations noted.
			Inspected internal documentation and determined information security and data access policies and controls were in place to prevent unauthorized access, alteration, disclosure, or destruction of important records.	No deviations noted.
117. The primary information assets within the ISMS are owned by the organization's customer and users. The organization serves as a	Control not relevant to meet the SOC 2 Criteria	DSP-06	Inquired of the Program Manager and determined the primary information assets are owned by the organizations users and the organization serves as a steward of that information in compliance with the published Terms of Service.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
steward of that information in compliance with the published Terms of Service.			Inspected relevant organizational documentation for GCP and determined the primary information assets are owned by the organizations users and that the organization serves as a steward of that information in compliance with the published Terms of Service.	No deviations noted.
118. The organization only processes user data in accordance with the applicable data processing terms and does not process user data for any other purpose.	P1.1, P3.1, P4.1	DSP-08, DSP-09, DSP-10, DSP-11, DSP-12, DSP-16	Inquired of the Program Manager and determined that customer data was only processed in accordance with the data processing terms and not for any other purpose.	No deviations noted.
			Inquired of Product Counsel Program Manager and determined Counsel reviewed new products and features prior to launch to confirm products and services were designed to only process customer data in accordance with the data processing addendum and not for any other purpose.	No deviations noted.
			Inspected the Cloud Data Processing and Security Terms and determined that Google only processed customer data in accordance with the applicable data processing terms and not for any other purpose.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a user upload data to Google Cloud Platform Services and determined that Google did not use the customer provided content for purposes not specified in the data processing addendum (e.g., advertising).	No deviations noted.
119. Customers of the organization's services are provided a mechanism to access, correct, and erase Customer Data created by their accounts, consistent with the functionality of the services.	P5.1, P5.2	DSP-11	Inquired of the Program Manager and determined that Customers of the organization's services were provided a mechanism to access, correct, and erase PII created by their accounts.	No deviations noted.
			Inspected the Google Cloud Data Processing Terms and relevant technical guides and determined that Customers of the organization's services were provided a mechanism to access, correct, and erase PII created by their accounts.	No deviations noted.
			Observed a Google Cloud Platform Console sample test transaction and determined users have the ability to access, correct, and erase PII created by their account.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the Google Workspace Data Processing Terms and relevant technical guides and determined that Google provided Customers with the ability to access, correct, and erase PII created by their user account.	No deviations noted.
			Observed a sample Google Workspace product and determined Customers have the ability to access, correct, and erase PII created by their account.	No deviations noted.
			Inspected Google Chrome Services Data Processing Terms and determined that Google provides Customers with the ability to access, correct, and erase PII created by their user account.	No deviations noted.
			Observed a Google Chrome sample test transaction and determined Customers have the ability to access, correct, and erase PII created by their account.	No deviations noted.
120. A service administrator is provided a mechanism to facilitate a service user's right to access, correct, and erase Customer Data pertaining	P5.1, P5.2	DSP-11	Inquired of the Program Manager and determined a Google service administrator was provided a mechanism to facilitate a Google service user's right to access, correct, and erase PII pertaining to the user.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
to the user, consistent with the functionality of the services.			Inspected the Data Processing Terms and Terms of Service and determined that Google provides the mechanism to facilitate customer's ability to access, correct and erase PII pertaining to the user.	No deviations noted.
			Observed a sample Google Workspace product and determined service administrators had a mechanism to facilitate a user's ability to access, correct, and erase PII pertaining to the user.	No deviations noted.
			Observed a sample GCP product and determined service administrators had a mechanism to facilitate a user's ability to access, correct, and erase PII pertaining to the user.	No deviations noted.
			Observed a sample Chrome product and determined service administrators had a mechanism to facilitate a user's ability to access, correct, and erase PII pertaining to the user.	No deviations noted.
			Observed a sample Maps product and determined service administrators had a mechanism to facilitate a user's ability to access, correct, and erase PII pertaining to the user.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
121. Where the organization is a data processor, the organization has policies regarding its obligations to customers' ability to access, correct and/or erase their user data.	P5.1, P5.2, P6.7, P7.1	DSP-11	Inquired of the Program Manager and determined the organization had policies regarding its obligations to customers' ability to access, correct, and/or erase their user data.	No deviations noted.
			Inspected relevant documentation and determined the organization had policies regarding its obligations to customers' ability to access, correct, and/or erase their user data.	No deviations noted.
122. The organization outlines its commitments to data protection in the event of subprocessing of user data. Commitments are made available to customers.	Control not relevant to meet the SOC 2 Criteria	DSP-13, DSP-14, DSP-17, STA-03, STA-04, STA-05, STA-12, STA-14	Inquired of the Program Manager and determined security measures, a commitment not to degrade security, and a commitment to data protection in the event of sub-processing of customer data were documented and made available to customers.	No deviations noted.
			Inspected the Cloud Data Processing Addendum (Customers) available publicly and determined security measures and a commitment not to degrade security were made available to customers.	No deviations noted.
			Inspected Service Level Agreement and determined performance measures and indicators such as system uptime were documented.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected Service Level Agreement and determined performance measures and indicators such as system uptime were documented.	No deviations noted.
			Inspected publicly available website and determined procedures had been established for Google Cloud Product service recovery and reporting of issues.	No deviations noted.
			Inspected publicly available website and determined procedures had been established for Google Workspace service recovery and reporting of issues.	No deviations noted.
			Inspected the Google Cloud Product Terms of Service agreement and determined Google's responsibilities and commitments to customers were documented.	No deviations noted.
			Inspected the Google Workspace Terms of Service agreement and determined Google's responsibilities and commitments to customers were documented.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
123. Where the organization is a data processor, the organization maintains and makes available a list of subprocessors and updates that list, as contractually required.	P6.1, P6.4	DSP-13, DSP-14, STA-01, STA-02, STA-07	Inquired of the Program Manager and determined that where the organization is a data processor, the organization maintained and made available a list of subprocessors and updated that list, as contractually required.	No deviations noted.
			Inspected Google Workspace's public-facing website and determined an updated list of all subprocessors was publicly available, as contractually required.	No deviations noted.
			Inspected Google Cloud's public-facing website and determined an updated list of all subprocessors was publicly available, as contractually required.	No deviations noted.
			Inspected Google Chrome's public-facing website and determined an updated list of all subprocessors was publicly available, as contractually required.	No deviations noted.
			Inspected a sample email notification and determined notice of subprocessor changes were sent to customers.	No deviations noted.
			Inspected a sample notification to customers from PSOs and determined customers were made aware of the subprocessors used for their project.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
124. 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.	CC9.2, C1.1	DSP-13, STA-07, STA-08, STA-10, STA-11, STA-12, STA-13, STA-14	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
125. The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.	CC6.1, C1.1, C1.2, P4.2, P4.3	DSP-16, DSP-17, IPY-02, IPY-04, UEM-13	Inquired of the Program Manager and determined procedures were in place to dispose of confidential information according to the data retention and deletion policies.	No deviations noted.
			Inspected the organization's internal policies and determined guidelines were established to govern the retention and deletion of user data.	No deviations noted.
			Inspected the deletion monitoring dashboard and configuration for a sample product and determined the monitoring dashboard was used to manage the timeliness of deletion of confidential information as outlined in the data retention and deletion policies.	No deviations noted.
			Inspected a sample product and determined data deletion tools verified that backup data was deleted following the configured retention period, as part of the deletion mechanism process.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
126. The organization has a policy to reduce the risk of compromise to its data and infrastructure from devices connected to internal networks.	Control not relevant to meet the SOC 2 Criteria	DSP-17, IAM-03, UEM-10	Inquired of the Program Manager and determined the organization had established a Network and Computer Security policy to reduce the risk of compromise to its data and infrastructure from devices connected to internal networks.	No deviations noted.
			Inspected Google's Network and Computer Security Policy and other relevant documentation, and determined the organization had established policies to reduce the risk of compromise to its data and infrastructure from devices connected to internal networks.	No deviations noted.
127. Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon in the contract, unless such notification is otherwise prohibited.	P6.1, P6.7	DSP-18	Inquired the Program Manager and determined that customers were notified of data requests from government agencies in accordance with the procedure and time period agreed upon in the contract, unless such notification was otherwise prohibited.	No deviations noted.
			Inspected the Google Cloud Platform Terms of Service and other publicly available documentation and determined they outlined the procedures the company followed to notify customers when disclosure of customer data was legally required.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected Google's internal website and determined Google had established mechanisms to ensure customers were notified in accordance with the terms of service when a disclosure of customer data was legally required.	No deviations noted.
			Inspected the configuration supporting the automatic creation of data requests within Google's internal tools to validate that data requests from government agencies are tracked and managed.	No deviations noted.
			Inspected a sample of disclosure requests and determined notification was sent to the customers in accordance with contractual requirements.	No deviations noted.
128. The organization specifies and documents the countries and/or data center locations in which customer data might possibly be stored and transferred.	Control not relevant to meet the SOC 2 Criteria	DSP-19	Inquired of the Program Manager and determined Google specifies and documents the countries in which PII might possibly be stored via a public-facing website and related documentation.	No deviations noted.
			Inspected Google's public-facing website and determined Google specifies and documents the locations where data will be stored.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
129. Where the organization is a data processor, the organization informs controllers of the basis for transferring user data between jurisdictions.	Control not relevant to meet the SOC 2 Criteria	DSP-19	Inquired of the Program Manager and determined when Google was a data processor, it informed controllers of the legal basis for transferring user data between jurisdictions.	No deviations noted.
			Inspected the relevant documentation and determined Google informed controllers of the legal basis for transferring user data between jurisdictions.	No deviations noted.
			Inspected the Admin Console and determined a method existed for data controllers to indicate their requirement to transfer data between geographical jurisdictions, as described in the Data Processing Terms.	No deviations noted.
			Inspected a sample communication to a GCP customer and determined the customer was notified of a change and has the opportunity to object to the processing of their data.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
130. Information security is managed by an executive who is dedicated to Security, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.	CC1.5	GRC-01, GRC-06	Inquired of the Program Manager and determined information security was managed by an executive who is dedicated to security and privacy, is independent of information technology responsibility, and may escalate security matters to the board level concerning security issues.	No deviations noted.
			Inspected the security organizational structure and determined an executive was dedicated to security and was independent of information technology responsibilities.	No deviations noted.
			Inspected the minutes of meeting and determined the Security team met with relevant personnel to discuss security issues and escalated security concerns to the board of directors, as necessary.	No deviations noted.
131. The organization conducts periodic Privacy risk assessments to identify and evaluate risks	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, A1.3	GRC-02	Inquired of the Program Manager and determined the organization conducted periodic privacy risk assessments to identify and evaluate risks related to the handling of user data.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
related to the handling of user data.			Inspected internal documentation and determined the organization had a formal risk assessment process that included policies and procedures for identification, evaluation, ownership, treatment, and acceptance of privacy risks.	No deviations noted.
			Inspected the risk assessment and determined the organization identified and evaluated risks related to the handling of user data periodically.	No deviations noted.
132. The organization has established a process to review and approve requests for policy exceptions.	CC2.1, CC2.2	GRC-04	-	-
133. The organization plans and coordinates system security-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users.	Control not relevant to meet the SOC 2 Criteria	GRC-06	Inquired of the Program Manager and determined Google plans and coordinates system security-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users.	No deviations noted.
			Inspected a list of system security-related audits and determined Google planned and coordinated system security-related audits.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a relevant documentation and determined Google planned and coordinated system security-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users.	No deviations noted.
			Inspected a sample system security-related audit and determined Google planned and coordinated the audit with the relevant stakeholders before conducting activities in order to reduce the impact on internal and consumer users.	No deviations noted.
134. The organization is an active participant in the security industry and maintains appropriate contacts with special interest groups, security forums, and professional associations.	Control not relevant to meet the SOC 2 Criteria	GRC-08	Inquired of the Program Manager and determined the organization was an active participant in the security industry and maintained appropriate contacts with special interest groups, security forums, and professional associations.	No deviations noted.
			Inspected internal and external sites and determined the organization was an active participant in the security industry and maintained appropriate contacts with special interest groups, security forums, and professional associations.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
135. Background checks are performed on new hires as permitted by local laws.	CC1.1, CC1.4	HRS-01	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.
136. The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	CC6.7	HRS-02, UEM-01, UEM-02, UEM-05, UEM-08, UEM-12, UEM-13	Inquired of the Program Manager and determined the organization maintained policies for securing mobile devices used to access corporate network and systems.	No deviations noted.
			Inspected relevant policies and documentation and determined the organization maintained policies for securing mobile devices used to access corporate network and systems.	No deviations noted.
137. The organization has security policies that require users to lock their workstations and mobile devices when unattended.	Control not relevant to meet the SOC 2 Criteria	HRS-03	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected internal policies and determined the organization required users to lock their workstations and mobile devices when unattended.	No deviations noted.
			Inspected the idle time configurations propagated to workstations and determined they were configured to enforce password standards.	No deviations noted.
			Performed on-site inspections for a sample of offices and determined that employees followed appropriate office security practices including securing any paper and removable media, and 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.
138. The organization has security policies and guidelines around office security practices, including securing any hard copy (printed)	Control not relevant to meet the SOC 2 Criteria	HRS-03	Inquired of the Program Manager and determined the organization had security policies to inform employees on appropriate office security practices including securing any paper documents and removable media.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
documents and removable media.			Inspected the organization's security policies and determined the organization had security policies to inform employees on appropriate office security practices including securing any paper documents and removable media.	No deviations noted.
			Observed a sample of offices and determined that employees followed appropriate office security practices including securing any paper and removable media.	No deviations noted.
139. Remote access to corporate machines requires a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate.	CC6.1, CC6.6	HRS-04, IAM-02, IAM-05, IAM-14, IAM-16	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
140. Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis upon submission of a termination request by Human Resources or a manager.	CC5.2, CC6.2, CC6.3	HRS-05, IAM-02, IAM-05, IAM-07, IAM-08, IAM-14, IAM-16	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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample alert from the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined that the failure was resolved in a timely manner.	No deviations noted.
			Inspected a sample of terminated users and determined that access to production machines, support tools, network devices, and corporate assets was automatically revoked by the automated tool within seven (7) days of the user's termination date.	No deviations noted.
141. New hires or internal transfers are required to go through an official recruiting process during which they are screened against detailed job descriptions and interviewed to assess competence.	CC1.3, CC1.4	HRS-06	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	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.
142. The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	CC9.2, C1.1	HRS-07, HRS-08, HRS-09	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.
			Inspected a sample of Google extended workforce personnel and determined they signed the confidentiality agreements as part of their service conditions.	No deviations noted.
143. The organization has established confidentiality agreements that are reviewed (by regional	CC9.2, C1.1	HRS-07, HRS-08, HRS-10	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
Employment Legal teams) and updated (by Google's regional Offer Letter teams), as needed.			Inspected the confidentiality agreements and determined they were reviewed and updated as needed by the organization.	No deviations noted.
144. The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	CC9.2, C1.1	HRS-07, HRS-08, HRS-12	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
145. Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	CC7.5	HRS-12, SEF-01, SEF-05, SEF-07	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.
146. The organization maintains formal user registration and de-registration procedures for	CC6.2, CC6.3	IAM-02, IAM-03, IAM-05, IAM-06, IAM-	Inquired of the Program Manager and determined the organization maintained formal user registration and de-registration procedures for granting and revoking access.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
granting and revoking access.		07, IAM-13, IAM-14, IAM-16	Inspected relevant documentation and determined the organization had formal procedures defining the appropriate use of corporate and production accounts.	No deviations noted.
			Inspected relevant documentation and determined the organization had formal procedures for granting and revoking user access to the corporate and production network.	No deviations noted.
			Inspected the relevant guidelines and determined organization maintained formal user de-registration procedures for revoking access for employee's leaving the company.	No deviations noted.
			Observed an attempt to grant user access to a group with the appropriate approval from the group administrator and determined access was granted.	No deviations noted.
			Observed an attempt to grant user access to a group without the appropriate approval from the group administrator and determined access was not granted.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a terminated user's access to production machines, support tools, network devices and corporate assets and determined access was automatically removed by the automated tool used to revoke access upon submission of a termination request.	No deviations noted.
147. Mechanisms are in place to detect attempts, and prevent connections to the organization's network by unauthorized devices.	CC6.1, CC6.2	IAM-02, IAM-04, IAM-05, IAM-14, IAM-16, IVS-09	Inquired of the Program Manager and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
			Inspected relevant documentation and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
			Inspected relevant configurations and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
			Observed a user with an authorized device attempt to connect to the Google network and determined the connection was successful.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
148. The organization has a password change system that enforces its password guidelines.	Control not relevant to meet the SOC 2 Criteria	IAM-02, IAM-15	Inquired of the Program Manager and determined Google has a password change system that enforces Google's password guidelines.	No deviations noted.
			Inspected relevant documentation and determined password guidelines were established.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the configuration for password change requirements and determined it enforces Google's password guidelines.	No deviations noted.
			Observed a user attempt to change their password and determined that it was successful when it met the password guidelines.	No deviations noted.
			Observed a user attempt to change their password and determined an error message was given when password standards were not aligned with password guidelines.	No deviations noted.
149. The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	CC1.1, CC1.5	IAM-03, IAM-08	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	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.
150. Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	CC6.2, CC6.3	IAM-03, IAM-08, IAM-10, IVS-05, IVS-06	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.
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.	
151. The organization separates duties of individuals by granting users access based on job responsibilities and least privilege, and limiting	CC5.1	IAM-04, IAM-05, IAM-08, IAM-09, IAM-12, IAM-14,	Inquired of the Program Manager and determined organization separated duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
access to only authorized users.		IAM-16, LOG-04, LOG-09	Inspected relevant policies and guidelines, and determined Google separates duties of individuals as necessary, by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	No deviations noted.
			Inspected the configurations within the source code management system and determined that the 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.
			Inspected a sample of user group reviews and determined access was approved by the group administrators and review the users' access rights at regular intervals to confirm access granted is based on job responsibilities, least privilege and segregation of duties.	No deviations noted.
			Observed an attempt to grant user access to a group based on job responsibilities and least privilege by an appropriate approver and determined access was granted.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed an attempt to grant user access to a group based on job responsibilities and least privilege without an appropriate approver and determined access was not granted.	No deviations noted.
			Inspected a sample system generated log for access to production machines, support tools, and network devices and determined access approvals and modifications to the access lists were recorded.	No deviations noted.
			Inquired of the Program Manager and determined the organization separated duties of individuals for GCNV by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	No deviations noted.
			Inspected the configurations within the source code management system and determined that the relevant access control list systems were configured to enforce approval from a group administrator prior to a user receiving access to GCNV production machines, support tools, and network devices.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
152. The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	CC2.2, CC7.3	IAM-12, LOG-03, LOG-04, LOG-05, LOG-13, SEF-01, SEF-02, SEF-03, SEF-05, SEF-06, SEF-07	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.
153. The organization has mechanisms in place to prevent deactivated or deleted user accounts	Control not relevant to meet the	IAM-13	Inquired of the Program Manager and determined Google prevents deactivated or deleted user accounts from being reassigned to new users.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
from being reassigned to new users.	SOC 2 Criteria		Inspected the relevant documentation and determined Google prevents deactivated or deleted user accounts from being reassigned to new users.	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 new account had a unique ID.	No deviations noted.
			Observed a user attempt to create a user account using an existing username and determined the system prevented a duplicate account from being created.	No deviations noted.
			Observed a user attempt to create a user account using a deactivated username and determined the system prevented a deactivated account from being created.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
154. Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	CC6.6	IAM-16, IVS-06	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.
155. The organization has an established policy to ensure portability and interoperability which is updated at least annually.	Control not relevant to meet the SOC 2 Criteria	IPY-01, IPY-02, IPY-03	Inquired of the Program Manager and determined that Google had an established policy to help ensure portability and interoperability of data.	No deviations noted.
			Inspected Google's relevant documentation and determined that Google had an established commitment to ensure portability and interoperability of data.	No deviations noted.
			Inspected Google's Cloud Data Processing Addendum and determined the policy was reviewed at least annually.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected Google's policy documentation and user guides and determined users could request their data in standard processable electronic formats to help ensure portability.	No deviations noted.
			Inspected a sample of applicable products and determined that Google provided functionality to help ensure portability and interoperability of user data.	No deviations noted.
156. The organization's network security policies and guidelines apply to both physical and virtual networks.	Control not relevant to meet the SOC 2 Criteria	IVS-01, IVS-04	Inquired of the Program Manager and determined the organization's network security policies were applied to both physical and virtual networks.	No deviations noted.
			Inspected internal documentation and determined the organization's network security policies were applied to both physical and virtual networks.	No deviations noted.
157. The organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting	Control not relevant to meet the SOC 2 Criteria	IVS-02	Inquired of the Program Manager and determined the organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
based on usage and system performance.			Inspected the applicable guidelines and procedures and determined the organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	No deviations noted.
			Inspected the internal dashboard for a GCP product and determined the organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	No deviations noted.
			Inquired of the Program Manager and determined the organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	No deviations noted.
			Inspected the applicable guidelines and procedures and determined the organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the internal dashboard for GCNV and determined the organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	No deviations noted.
158. The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	CC7.1	IVS-03, IVS-04, IVS-09, UEM-10, UEM-11	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.
			Inquired of the Program Manager and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the GCNV 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 GCNV network	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
159. The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/ or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	CC6.1	IVS-03, IVS-09, UEM-10	Inquired of the Program Manager and determined networks were segregated based on the types of services, users and information systems. Inquired and determined that networks are physically and/ or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	No deviations noted.
			Inspected internal documentation and determined networks were designed to be logically or physically segregated.	No deviations noted.
			Inspected configurations and determined networks used for migration and generation of virtual machines were physically and logically segregated from other networks.	No deviations noted.
			Inspected internal documentation and determined networks for the management of the infrastructure and for the operation of management consoles were separated.	No deviations noted.
			Inspected internal documentation and determined processes were defined to maintain separate development, testing and production environments.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected network diagrams and determined high-risk environments were designed to be physically and logically segregated from other networks.	No deviations noted.
			Inquired of the Program Manager and determined GCNV networks were segregated based on the types of services, users and information systems. Inquired and determined that networks are physically and/ or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	No deviations noted.
			Inspected internal documentation and determined GCNV networks were designed to be logically or physically segregated.	No deviations noted.
			Inspected network architecture diagrams and determined GCNV networks used for migration and generation of virtual machines were physically and logically segregated from other networks.	No deviations noted.
			Inspected internal documentation and determined GCNV networks for the management of the infrastructure and for the operation of management consoles were separated.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected network architecture diagrams and determined high-risk environments for GCNV were designed to be physically and logically segregated from other networks.	No deviations noted.
160. The organization has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	Control not relevant to meet the SOC 2 Criteria	IVS-06	Inquired of the Program Manager and determined Google has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	No deviations noted.
			Inspected the relevant documentation and determined Google has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	No deviations noted.
			Performed test transactions and determined Google has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	No deviations noted.
			Observed a user attempt to create a new user with a username belonging to an active user and determined that duplicate IDs cannot be created.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Observed a user attempt to create a new user with a username belonging to a terminated user and determined that duplicate IDs cannot be created.	No deviations noted.
			Observed a user share a file with another user and determined that access to the file can be granted and revoked.	No deviations noted.
			Inspected the web browser settings in accessing the cloud service and determined the session ID connection is encrypted and longer than 128 bits to help ensure secure segmentation and connection.	No deviations noted.
161. The organization provides customers with information regarding default encryption methods used to protect user data. Additional applications of cryptographic protections	Control not relevant to meet the SOC 2 Criteria	IVS-07	Inquired of the Program Manager and determined the organization provided its customers with information regarding default encryption methods used to protect customer data and additional applications of cryptographic protections were documented and shared through public sites.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
are documented and shared through public sites.			Inspected publicly available documentation and determined the organization provided its customers with information regarding default encryption methods used to protect customer data and additional applications of cryptographic protections were documented and shared through public sites.	No deviations noted.
162. The organization has implemented mechanisms to protect the production environment from denial of service attacks.	CC7.2	IVS-08, IVS-09	Inquired of the Program Manager and the Security Reliability Engineer and determined there were mechanisms in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
			Inspected the documentation for mechanisms that are used to protect against denial of service attacks and determined they were in place to protect the production environment.	No deviations noted.
			Inspected playbooks used by the incident management teams and determined mechanisms were in place to classify, escalate and triage denial of service attacks.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the DOS server configuration and determined configurations were in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
			Inspected a sample of denial of service attacks and determined mechanisms were in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
			Inspected the dashboards for a sample of in-scope applications and determined monitoring mechanisms were in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
163. The organization monitors its networks and systems for threats to information security.	Control not relevant to meet the SOC 2 Criteria	IVS-09, LOG-09	Inquired of the Security Engineering Manager and determined the organization monitors its networks and systems for threats to information security.	No deviations noted.
			Inspected Google's risk assessment and determined the organization managed threats to information security by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of Google products and services.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample log configuration and determined log sources were monitored and maintained.	No deviations noted.
			Inspected a sample of alerts and determined configurations appropriately monitored events and generated security alerts in the SIEM tool when the pre-defined threshold was met or exceeded.	No deviations noted.
			Inspected the dashboard of monitoring tools and determined that alerts related to information security were monitored.	No deviations noted.
164. Security event logs are protected and access is restricted to authorized personnel.	CC6.1, CC6.2	IVS-09, LOG-09	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample of members with access to audit logs and determined they were appropriate to have access to audit logs.	No deviations noted.
			Inspected a sample semiannual user access review and determined access to audit logs was reviewed on a periodic basis and that appropriate action was taken to resolve inappropriate access, if applicable.	No deviations noted.
165. Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	CC6.8, CC7.2, CC7.3, CC7.4, CC7.5, CC8.1, A1.1	LOG-01, LOG-02, LOG-03, LOG-04, LOG-05, LOG-07, LOG-09, LOG-10, LOG-13, SEF-01, SEF-05, SEF-06, SEF-07	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			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.
166. The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	CC6.8, CC7.1, CC7.3, A1.1	LOG-01, LOG-02, LOG-03, LOG-04, LOG-05, LOG-09, LOG-10, LOG-11, LOG-13, SEF-01, SEF-05, SEF-06, SEF-07	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
167. Audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts.	Control not relevant to meet the SOC 2 Criteria	LOG-02, LOG-04, LOG-05, LOG-07, LOG-08, LOG-09, LOG-10, LOG-11, LOG-13	Inquired of Security Engineering Manager and determined audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts, providing forensic accountability to detect and investigate potential incidents or anomalies.	No deviations noted.
			Inspected relevant documentation and determined audit logs are retained for auditable events, such as privileged user access activities, authorized access attempts, and unauthorized access attempts.	No deviations noted.
			Inspected the system configuration related to audit logs and determined log files are not modifiable.	No deviations noted.
			Inspected a sample audit log and determined it was retained for auditable events, such as privileged user access activities, authorized access attempts, and unauthorized access attempts.	No deviations noted.
			Inspected a sample monitoring alert and determined the availability of logs was monitored by the Security Surveillance Team.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample audit log of historical auditable events and determined log data is retained according to the retention policy, including content of the log record and retention time.	No deviations noted.
			Inquired of Security Engineering Manager and determined audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts, providing forensic accountability to detect and investigate potential incidents or anomalies.	No deviations noted.
			Inspected the system configuration related to audit logs and determined logs are retained for auditable events, such as privileged user access activities, authorized access attempts, and unauthorized access attempts.	No deviations noted.
168. At a minimum, security event logs must include the following: user ID, event type, timestamp, success/failure indication, event origination, and affected data/resource	Control not relevant to meet the SOC 2 Criteria	LOG-02, LOG-07, LOG-08	Inquired of Security Engineering Manager and determined, at a minimum, audit logs must include the following: user ID, event type, timestamp, success/failure indication, event origination, and affected data/resource identifier. Audit logs are retained for a minimum of one year.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
identifier. Security event logs are retained for a minimum of one (1) year.			Inspected relevant documentation and determined audit logs must include the following: user ID, event type, timestamp, success/failure indication, event origination, and affected data/resource identifier, and determined audit logs are retained for a minimum of one year.	No deviations noted.
			Inspected a sample audit log of historical auditable events and determined log data is retained according to the retention policy, where data logs include the following attributes: user ID, event type, timestamp, success/failure indication, event origination, and affected data/resource identifier, and are retained for a minimum of one year.	No deviations noted.
169. Security event logs are replicated and securely maintained.	Control not relevant to meet the SOC 2 Criteria	LOG-02, LOG-09	Inquired of the Program Manager and determined audit log backups are securely maintained.	No deviations noted.
			Inspected relevant documentation and determined audit log backups are retained for auditable events according to the organization's retention policy and access to audit log backups is restricted to appropriate users.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected replication configurations for audit log backups and determined audit logs were configured to replicate across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	No deviations noted.
			Inspected a sample of one and determined log data is replicated across distinct, geographically dispersed processing facilities to support service redundancy, and availability and is retained according to the retention policy.	No deviations noted.
			Inspected the monitoring dashboard and determined audit log replications are monitored.	No deviations noted.
			Inspected the system configuration related to audit log backups and determined log files are not modifiable.	No deviations noted.
			Inspected a sample user access review and determined the administrator group which grants access to audit log backups was reviewed on a periodic basis.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
170. The organization provides internal personnel (employees and extended workforce) with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the responsible team(s).	CC7.3, CC7.4, P6.3	LOG-03, LOG-10, LOG-13, SEF-01, SEF-07	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample of incident tickets and determined the incident response team quantified and monitored incidents.	No deviations noted.
171. The organization provides external users with mechanisms to report security issues, incidents and concerns.	CC2.3	LOG-03, LOG-13, SEF-01, SEF-02, SEF-03, SEF-07	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.
172. Internal system clocks are synchronized to atomic clocks and GPS.	Control not relevant to meet the	LOG-06	Inquired of the Program Manager and determined that internal system clocks were synchronized to atomic clocks and GPS.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
	SOC 2 Criteria		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.
			Inquired of the Program Manager and determined that internal system clocks for GCNV were synchronized to atomic clocks and GPS.	No deviations noted.
			Inspected public documentation and determined that internal system clocks for GCNV were synchronized to atomic clocks and GPS.	No deviations noted.
			Inspected the relevant configurations and determined that internal system clocks for GCNV were synchronized to atomic clocks and GPS.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected evidence showing the synchronization of internal system clocks for GCNV to atomic clocks and GPS.	No deviations noted.
173. The organization maintains a framework that defines how to organize a response to security and privacy incidents.	CC7.3, CC7.4, P6.3	SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, SEF-06, SEF-07	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.
174. The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	CC7.3, CC7.4, P6.3, P6.6	SEF-07, SEF-08	Inquired of the Program Manager and determined the organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	No deviations noted.
			Inspected relevant documentation and determined procedures existed for users to prepare, report and investigate security and privacy incidents.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected the Cloud Data Processing Amendment and determined policies and procedures existed to notify customers of an incident in a timely manner and in accordance with applicable laws.	No deviations noted.
			Inspected a sample of data incidents and determined customers were notified of data incidents in a timely manner when required by applicable laws or contractual agreements.	No deviations noted.
			Inspected the public dashboards and tools available to customers and determined customers were notified of outages and incidents that impact relevant services.	No deviations noted.
175. The organization establishes designated legal counsel and Government Affairs officials in order to maintain appropriate contacts with law enforcement authorities.	Control not relevant to meet the SOC 2 Criteria	SEF-08	Inquired of the Program Manager and determined the organization established designated legal counsel and Government Affairs officials in order to maintain appropriate contacts with law enforcement authorities.	No deviations noted.
			Inspected internal websites and policies and determined the organization established designated legal counsel and Government Affairs officials in order to maintain appropriate contacts with law enforcement authorities.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
176. The organization provides information pertaining to the shared responsibilities of both itself and the cloud service customer.	Control not relevant to meet the SOC 2 Criteria	STA-01, STA-02, STA-03, STA-04, STA-05, STA-06	Inquired of the Program Manager and determined that the organization provided information pertaining to the shared responsibilities of both itself and the cloud service customer.	No deviations noted.
			Inspected the product agreements and terms of service and determined that the organization provided information pertaining to the shared responsibilities of both itself and the cloud service customer.	No deviations noted.
177. Customer responsibilities are described on the organization's product websites or in system documentation.	CC2.2, CC2.3	STA-01, STA-02, STA-03, STA-04, STA-05, STA-09	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.
178. Subprocessor perfomance is regularly assessed and monitored	CC9.2	STA-02	Inquired of the Program Manager and determined subprocessor performance was regularly assessed and monitored via periodic business reviews.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
via periodic business reviews			Inspected documentation for a sample of subprocessors and determined that subprocessor performance was regularly assessed and monitored via periodic business reviews.	No deviations noted.
179. Cloud Subprocessor security and privacy risk is assessed via periodic assessment of sub-processor control environment.	CC9.2, P6.1, P6.4	STA-02, STA-06, STA-08, STA-12, STA-13, STA-14	Inquired of the Program Manager and determined Cloud subprocessor security and privacy risk was assessed via periodic assessment of subprocessor control environment.	No deviations noted.
			Inspected documentation of a review for a sample of subprocessors and determined that assessments of their security and privacy controls were performed on a periodic basis.	No deviations noted.
180. The organization maintains an up-to-date, accurate client device inventory	Control not relevant to meet the SOC 2 Criteria	STA-07, UEM-04	Inquired of the Program Manager and determined the organization maintains an up-to-date and accurate client device inventory.	No deviations noted.
			Inspected documentation and determined the organization defined policies that ensure that up-to-date and accurate client device inventory is maintained.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected code configuration and determined that the inventory system maintains an up-to-date and accurate client device inventory.	No deviations noted.
			Observed that the data center asset tracking software was updated when network equipment was removed.	No deviations noted.
			Observed that the data center asset tracking software was updated when network equipment was reinserted.	No deviations noted.
			Observed that the data center asset tracking software was updated when machine part was removed.	No deviations noted.
			Observed that the data center asset tracking software was updated when machine part was reinserted.	No deviations noted.
			Inspected a sample of machines from the inventory system and determined the machines existed in the data center.	No deviations noted.
			Inspected a sample of machines from data center inspections and determined the machines were accounted for in the inventory system.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
181. The organization requires subprocessors to meet security and privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are enforced via the “Subprocessor Data Protection Agreement (SDPA)” addendum to contractual agreements or other data processing terms.	CC9.2, C1.1, P6.1, P6.4, P6.5, P6.6	STA-11, STA-12	Inquired of the Program Manager and determined the organization required subprocessors to meet security and privacy requirements for safeguarding user data and the requirements were enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements.	No deviations noted.
			Observed the addendum template and determined it defined the security and privacy obligations that subprocessors must meet to satisfy the organization's obligation regarding customer data.	No deviations noted.
			Inspected a sample of subprocessors and determined that the subprocessors had a signed SDPA in place in addition to their contractual agreements to enforce security and privacy requirements.	No deviations noted.
			Inspected the addendum template and determined that appropriate exception handling procedures for service or product issues related to vendors were in place.	No deviations noted.
182. The organization has policies and guidelines that govern third-party relationships.	CC9.2	STA-12	Inquired of the Program Manager and determined the organization developed policies and guidelines that govern third party relationships.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected internal documentation and determined policies and guidelines were in place to govern third party relationships.	No deviations noted.
183. The organization has implemented mechanisms to protect its information assets against malicious activity (e.g. malware, spam, phishing).	CC6.8	TVM-02, TVM-04, UEM-09	Inquired of the Program Manager and determined the organization has implemented mechanisms to protect its information assets against malicious activity.	No deviations noted.
			Inspected Google's internal guidelines and determined the organization has implemented mechanisms to protect its information assets against malicious activity.	No deviations noted.
			Inspected the antivirus and antimalware mechanisms and determined that the tools were in place to protect the organization's information assets.	No deviations noted.
			Inspected internal documentation and determined antivirus software in place was configured to have a function to roll-back to a previous state in case of malfunction of an anti-virus system update.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
184. The organization has established mechanisms governing the configuration and security of corporate-managed devices providing privileged access.	CC6.1	UEM-01, UEM-02, UEM-03, UEM-05, UEM-08, UEM-10, UEM-12, UEM-13	Inquired of the Program Manager and determined the organization has established mechanisms governing the configuration and security of corporate-managed devices providing privileged access.	No deviations noted.
			Inspected relevant documentation and determined that policies are in place to govern the device management, security, and baseline requirements of corporate-managed mobile devices providing privileged access.	No deviations noted.
			Inspected relevant documentation and determined that policies are in place to govern the use of encryption for corporate-managed mobile devices providing privileged access.	No deviations noted.
			Inspected relevant documentation and determined policies are in place for access protection and identity management for corporate-managed mobile devices.	No deviations noted.
			Inspected relevant policies and documentation and determined unofficial operating systems are prohibited on corporate-managed mobile devices.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected relevant policies and documentation and determined requirements for BYOD mobile devices for use in the corporate environment are established.	No deviations noted.
			Inspected the configuration for corporate-managed devices with privileged access and determined the organization implemented access protection, identity, and authorization management protections.	No deviations noted.
			Inspected the device settings on a corporate-managed device with privileged access and determined access protection, identity, and authorization management protections are implemented as configured.	No deviations noted.
185. The organization has a security guideline that requires users to lock their workstations and mobile devices when unattended. Workstations are configured to initiate a password protected screen-saver after 15	CC6.1	UEM-06	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
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.
186. The organization has guidelines in place for the management and use of removable media.	Control not relevant to meet the SOC 2 Criteria	UEM-11	Inquired of the program manager and determined the organization had established procedures in place for the management and use of removable media.	No deviations noted.
			Inspected relevant policies and guidelines and determined Google had established procedures in place for the management and use of removable media.	No deviations noted.
187. The organization prohibits the use of removable media for the storage of PII and SPII	CC6.7, P4.3	UEM-11	Inquired of the Program Manager and determined PII and SPII on removable media leaving Google facilities was approved and encrypted.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
unless the data has been encrypted.			Inspected relevant policies and determined Google outlined and communicated the process for the secure handling and transportation of customer data.	No deviations noted.
			Inspected the ticketing tool and determined requests to use removable media were approved under the condition that the removable media was encrypted.	No deviations noted.
188. The organization has implemented Data Loss Prevention (DLP) mechanisms to detect data loss originating from employee accounts that access corporate ("corp") services.	Control not relevant to meet the SOC 2 Criteria	UEM-11	Inquired of the Program Manager and determined the Organization has implemented Data Loss Prevention mechanisms to detect data loss originating from employee accounts that access corporate services.	No deviations noted.
			Inspected Google's internal documentation and determined there are guidelines used by Google to detect data loss originating from employee accounts that access corporate services and perform cause analysis, and triage the security incidents.	No deviations noted.
			Inspected a sample configuration to ensure that mechanisms are in place to detect data loss originating from employee accounts that access corporate services.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	CCM Criteria Reference	Tests Performed by EY	Results
			Inspected a sample of alerts for events related to security, availability, privacy and confidentiality and determined the alerts were generated and mitigated accordingly.	No deviations noted.

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
CC1.1 - COSO Principle 1		
CC1.1	28, 53, 111, 135, 149	The entity demonstrates a commitment to integrity and ethical values.
CC1.2 - COSO Principle 2		
CC1.2	12	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3 - COSO Principle 3		
CC1.3	2, 4, 54, 141	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4 - COSO Principle 4		
CC1.4	4, 28, 135, 141	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5 - COSO Principle 5		
CC1.5	12, 26, 54, 130, 149	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.1 - COSO Principle 13		
CC2.1	24, 45, 67, 132	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2 - COSO Principle 14		
CC2.2	23, 24, 28, 54, 65, 115, 132, 152, 177	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3 - COSO Principle 15		
CC2.3	5, 6, 78, 115, 171, 177	The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.1 - COSO Principle 6		

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
CC3.1	27, 32, 33, 54, 131	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2 - COSO Principle 7		
CC3.2	27, 32, 33, 51, 66, 76, 131	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3 - COSO Principle 8		
CC3.3	27, 32, 33, 51, 131	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4 - COSO Principle 9		
CC3.4	27, 32, 33, 131	The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.1 - COSO Principle 16		
CC4.1	22, 25, 26, 56	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2 - COSO Principle 17		
CC4.2	25, 26	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
CC5.1 - COSO Principle 10		
CC5.1	21, 27, 33, 131, 151	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2 - COSO Principle 11		
CC5.2	3, 21, 27, 30, 33, 77, 112, 131, 140	The entity also selects and develops general control activities over technology to support the achievement of objectives.

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
CC5.3 - COSO Principle 12		
CC5.3	22, 23, 25, 30, 34, 43	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.1		
CC6.1	1, 18, 35, 39, 72, 76, 82, 86, 87, 89, 90, 92, 107, 108, 109, 125, 139, 147, 159, 164, 184, 185	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2		
CC6.2	3, 19, 64, 107, 140, 146, 147, 150, 164	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3		
CC6.3	3, 19, 140, 146, 150	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
CC6.4		
CC6.4	11, 96, 97, 98, 99, 100, 101, 103, 104	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5		

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
CC6.5	94	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6		
CC6.6	3, 88, 89, 90, 91, 139, 154	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7		
CC6.7	57, 73, 75, 81, 85, 86, 88, 89, 99, 105, 136, 187	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8		
CC6.8	51, 80, 165, 166, 183	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
CC7.1		
CC7.1	17, 51, 57, 58, 70, 158, 166	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2		
CC7.2	27, 51, 70, 71, 114, 162, 165	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3		
CC7.3	70, 71, 114, 152, 165, 166, 170, 173, 174	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
CC7.4		
CC7.4	62, 70, 71, 114, 165, 170, 173, 174	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5		
CC7.5	34, 70, 71, 145, 165	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.1		
CC8.1	35, 36, 45, 46, 47, 60, 73, 74, 165	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.1		
CC9.1	20, 44, 52, 61	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2		
CC9.2	53, 124, 142, 143, 144, 178, 179, 181, 182	The entity assesses and manages risks associated with vendors and business partners.
A1.1		
A1.1	62, 64, 165, 166	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2		
A1.2	20, 52, 61, 62, 64, 68, 113	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
A1.3		
A1.3	20, 27, 52, 61, 62, 71, 131	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
C1.1		
C1.1	1, 2, 5, 37, 48, 53, 72, 114, 124, 125, 142, 143, 144, 181	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2		
C1.2	1, 125	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
P1.1		
P1.1	15, 38, 118	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.
P2.1		
P2.1	15, 38	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.
P3.1		
P3.1	15, 48, 118	Personal information is collected consistent with the entity's objectives related to privacy.

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
P3.2		
P3.2	15	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.
P4.1		
P4.1	15, 72, 118	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.
P4.2		
P4.2	1, 15, 38, 125	The entity retains personal information consistent with the entity's objectives related to privacy.
P4.3		
P4.3	1, 38, 94, 125, 187	The entity securely disposes of personal information to meet the entity's objectives related to privacy.
P5.1		
P5.1	119, 120, 121	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.
P5.2		
P5.2	119, 120, 121	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.
P6.1		

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
P6.1	13, 123, 127, 179, 181	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.
P6.2		
P6.2	14	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.
P6.3		
P6.3	9, 71, 170, 173, 174	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.
P6.4		
P6.4	13, 123, 179, 181	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.
P6.5		
P6.5	9, 181	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.
P6.6		
P6.6	174, 181	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.
P6.7		

SOC 2 Criteria to Controls Mapping

SOC 2

Criteria	Controls List	Criteria
P6.7	16, 121, 127	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.
P7.1		
P7.1	15, 121	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.
P8.1		
P8.1	7, 8, 10, 31	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
Audit and Assurance Policy and Procedures		
AandA-01	21, 22, 23, 24	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.
AandA-02	21, 25, 26	Conduct independent audit and assurance assessments according to relevant standards at least annually.
AandA-03	21, 25, 26, 27	Perform independent audit and assurance assessments according to risk-based plans and policies.
AandA-04	21, 25, 28, 29, 30	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.
AandA-05	21, 25, 26	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.
AandA-06	21, 27, 31, 32, 33	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.
Application and Interface Security		
AIS-01	22, 23, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.
AIS-02	34, 35, 36, 37, 45, 46, 47, 48	Establish, document and maintain baseline requirements for securing different applications.
AIS-03	22, 27, 28, 29, 32, 33, 49, 50, 51, 52, 53, 54, 55, 56	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
AIS-04	22, 23, 34, 35, 36, 37, 45, 46, 47, 48, 57, 58, 59	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.
AIS-05	34, 35, 36, 37, 45, 46, 47, 48, 57, 58	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.
AIS-06	34, 35, 36, 37, 45, 46, 47, 51, 60	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.
AIS-07	34, 35, 36, 37, 45, 46, 47, 51, 60	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.
Business Continuity Management and Operational Resilience		
BCR-01	52, 61, 62	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.
BCR-02	27, 32, 33, 52, 61, 62, 63, 64	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.
BCR-03	23, 24, 27, 28, 32, 33, 52, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.
BCR-04	52, 61	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.
BCR-05	24, 30, 52, 61, 62, 65, 66, 67	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
BCR-06	52, 61	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.
BCR-07	52, 61, 71	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.
BCR-08	61, 62, 72	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.
BCR-09	52, 61	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.
BCR-10	52, 61	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.
BCR-11	62, 64, 68, 69, 70	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.
Change Control and Configuration Management		
CCC-01	22, 30, 34, 35, 36, 45, 46, 60, 73, 74	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.
CCC-02	34, 35, 36, 37, 45, 46, 47, 48, 60	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.
CCC-03	30, 34, 35, 36, 45, 46, 60, 73, 74	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).
CCC-04	34, 35, 38, 45, 46, 73, 75, 76, 77	Restrict the unauthorized addition, removal, update, and management of organization assets.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
CCC-05	30, 34, 35, 36, 45, 46, 53, 60, 73, 74, 78	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.
CCC-06	34, 47	Establish change management baselines for all relevant authorized changes on organization assets.
CCC-07	21, 28, 30, 34, 36, 37, 45, 46, 47, 48, 60, 66, 73, 79, 80	Implement detection measures with proactive notification in case of changes deviating from the established baseline.
CCC-08	34, 36	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.
CCC-09	34, 35, 36	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.
Cryptography Encryption and Key Management		
CEK-01	22, 23, 24, 81, 82, 83, 84, 85, 86, 87, 88, 89	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.
CEK-02	81, 82	Define and implement cryptographic, encryption and key management roles and responsibilities.
CEK-03	81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.
CEK-04	72, 81, 82	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.
CEK-05	34, 45, 46, 60, 81, 82, 83, 93	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
CEK-06	24, 27, 34, 81, 82, 83	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.
CEK-07	27, 32, 33, 81	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.
CEK-08	81	CSPs must provide the capability for CSCs to manage their own data encryption keys.
CEK-09	21, 25, 81	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).
CEK-10	81, 82	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.
CEK-11	81, 82	Manage cryptographic secret and private keys that are provisioned for a unique purpose.
CEK-12	81, 82	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.
CEK-13	81, 82	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.
CEK-14	81, 82	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
CEK-15	81, 82	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.
CEK-16	81, 82	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.
CEK-17	81, 82	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.
CEK-18	81, 82	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.
CEK-19	81, 82	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstances, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.
CEK-20	27, 81, 82	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.
CEK-21	29, 81, 82	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.
Datacenter Security		

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
DCS-01	22, 94	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.
DCS-02	22, 39, 75, 95, 96	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.
DCS-03	22, 23, 95, 97, 98, 99, 100, 101, 102, 103, 104	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.
DCS-04	22, 75, 94	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.
DCS-05	32, 72, 76, 105	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.
DCS-06	75, 105	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.
DCS-07	75, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.
DCS-08	105, 106, 107, 108, 109	Use equipment identification as a method for connection authentication.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
DCS-09	95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 110	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.
DCS-10	75, 95, 96, 98, 99, 100, 101, 102, 103, 104	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.
DCS-11	28, 53, 67, 100, 101, 111	Train datacenter personnel to respond to unauthorized ingress or egress attempts.
DCS-12	27, 64, 68	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.
DCS-13	64, 68, 69, 100, 112	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.
DCS-14	64, 68, 69, 112	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.
DCS-15	27, 62, 64, 68, 69, 112, 113	Keep business-critical equipment away from locations subject to high probability for environmental risk events.
Data Security and Privacy Lifecycle Management		
DSP-01	22, 23, 27, 39, 40, 72, 76	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.
DSP-02	94	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
DSP-03	37, 41, 48, 72, 114	Create and maintain a data inventory, at least for any sensitive data and personal data.
DSP-04	27, 32, 33, 72	Classify data according to its type and sensitivity level.
DSP-05	21, 22, 23, 37, 48, 67, 76, 78, 115, 116	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.
DSP-06	22, 72, 76, 106, 117	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.
DSP-07	30, 34, 35, 36, 37, 45, 46, 60, 79	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.
DSP-08	28, 30, 34, 35, 36, 37, 41, 45, 46, 48, 118	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.
DSP-09	27, 33, 48, 118	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.
DSP-10	27, 29, 32, 33, 40, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 107, 118	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.
DSP-11	42, 78, 118, 119, 120, 121	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.
DSP-12	29, 118	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
DSP-13	122, 123, 124	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.
DSP-14	122, 123	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.
DSP-15	72, 74, 76	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.
DSP-16	29, 62, 72, 76, 94, 118, 125	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.
DSP-17	23, 24, 39, 43, 66, 72, 81, 83, 84, 85, 92, 116, 122, 125, 126	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.
DSP-18	127	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.
DSP-19	62, 128, 129	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.
Governance, Risk Management and Compliance		
GRC-01	21, 22, 23, 24, 27, 33, 130	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
GRC-02	23, 27, 32, 33, 41, 131	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.
GRC-03	22, 27, 33	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.
GRC-04	23, 132	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.
GRC-05	21, 23	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.
GRC-06	21, 24, 25, 27, 32, 33, 54, 130, 133	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.
GRC-07	21, 25, 27, 29, 32, 33	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.
GRC-08	134	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.
Human Resources		
HRS-01	135	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
HRS-02	22, 23, 24, 76, 86, 111, 136	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.
HRS-03	22, 23, 24, 28, 111, 137, 138	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.
HRS-04	22, 23, 24, 86, 139	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.
HRS-05	76, 77, 140	Establish and document procedures for the return of organization-owned assets by terminated employees.
HRS-06	77, 141	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.
HRS-07	28, 53, 111, 142, 143, 144	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.
HRS-08	28, 53, 111, 142, 143, 144	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.
HRS-09	24, 28, 53, 111, 142	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.
HRS-10	143	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.
HRS-11	28	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
HRS-12	53, 55, 111, 144, 145	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.
HRS-13	24, 28	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.
Identity and Access Management		
IAM-01	22, 23, 43	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.
IAM-02	22, 23, 24, 39, 77, 87, 90, 107, 108, 109, 139, 140, 146, 147, 148	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.
IAM-03	43, 107, 108, 126, 146, 149, 150	Manage, store, and review the information of system identities, and level of access.
IAM-04	39, 43, 107, 147, 151	Employ the separation of duties principle when implementing information system access.
IAM-05	24, 39, 43, 90, 107, 108, 139, 140, 146, 147, 151	Employ the least privilege principle when implementing information system access.
IAM-06	43, 87, 107, 146	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.
IAM-07	43, 77, 140, 146	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
IAM-08	39, 77, 140, 149, 150, 151	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.
IAM-09	34, 39, 43, 45, 114, 151	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.
IAM-10	39, 53, 82, 88, 90, 107, 114, 150	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.
IAM-12	34, 39, 71, 114, 151, 152	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.
IAM-13	107, 146, 153	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.
IAM-14	39, 43, 77, 88, 90, 91, 107, 108, 109, 139, 140, 146, 147, 151	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.
IAM-15	22, 23, 89, 109, 148	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.
IAM-16	39, 77, 88, 90, 91, 107, 108, 109, 139, 140, 146, 147, 151, 154	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.
Interoperability and Portability		

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
IPY-01	22, 23, 59, 67, 155	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.
IPY-02	38, 59, 78, 125, 155	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.
IPY-03	38, 59, 84, 155	Implement cryptographically secure and standardized network protocols for the management, import and export of data.
IPY-04	38, 42, 59, 78, 125	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy
Infrastructure and Virtualization Security		
IVS-01	22, 23, 79, 80, 156	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.
IVS-02	61, 62, 70, 71, 157	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
IVS-03	84, 85, 87, 88, 89, 91, 114, 158, 159	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.
IVS-04	47, 60, 79, 80, 156, 158	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.
IVS-05	74, 114, 150	Separate production and non-production environments.
IVS-06	85, 90, 107, 150, 154, 160	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.
IVS-07	83, 84, 85, 89, 92, 161	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.
IVS-08	91, 114, 162	Identify and document high-risk environments.
IVS-09	91, 114, 147, 158, 159, 162, 163, 164	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.
Logging and Monitoring		
LOG-01	22, 23, 24, 114, 165, 166	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.
LOG-02	114, 165, 166, 167, 168, 169	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.
LOG-03	71, 78, 114, 152, 165, 166, 170, 171	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
LOG-04	39, 71, 151, 152, 165, 166, 167	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.
LOG-05	71, 114, 152, 165, 166, 167	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.
LOG-06	172	Use a reliable time source across all relevant information processing systems.
LOG-07	22, 23, 114, 165, 167, 168	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.
LOG-08	114, 167, 168	Generate audit records containing relevant security information.
LOG-09	39, 151, 163, 164, 165, 166, 167, 169	The information system protects audit records from unauthorized access, modification, and deletion.
LOG-10	71, 81, 82, 83, 114, 165, 166, 167, 170	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.
LOG-11	81, 82, 83, 114, 166, 167	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.
LOG-12	100, 101, 102, 103, 104, 110	Monitor and log physical access using an auditable access control system.
LOG-13	71, 78, 114, 152, 165, 166, 167, 170, 171	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.
Security Incident Management, E-Discovery, and Cloud Forensics		

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
SEF-01	22, 23, 24, 51, 66, 71, 114, 145, 152, 165, 166, 170, 171, 173	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.
SEF-02	22, 23, 24, 51, 66, 71, 152, 171, 173	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.
SEF-03	61, 71, 78, 152, 171, 173	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.
SEF-04	61, 71, 173	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.
SEF-05	71, 114, 145, 152, 165, 166, 173	Establish and monitor information security incident metrics.
SEF-06	51, 71, 104, 114, 152, 165, 166, 173	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.
SEF-07	24, 71, 78, 114, 145, 152, 165, 166, 170, 171, 173, 174	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.
SEF-08	174, 175	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.
Supply Chain Management, Transparency and Accountability		

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
STA-01	22, 23, 44, 123, 176, 177	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.
STA-02	44, 123, 176, 177, 178, 179	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.
STA-03	122, 176, 177	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.
STA-04	122, 176, 177	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.
STA-05	122, 176, 177	Review and validate SSRM documentation for all cloud service offerings the organization uses.
STA-06	21, 25, 176, 179	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.
STA-07	105, 123, 124, 180	Develop and maintain an inventory of all supply chain relationships.
STA-08	21, 124, 179	CSPs periodically review risk factors associated with all organizations within their supply chain.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
STA-09	78, 177	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy
STA-10	42, 78, 124	Review supply chain agreements between CSPs and CSCs at least annually.
STA-11	21, 22, 25, 26, 53, 124, 181	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.
STA-12	122, 124, 179, 181, 182	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.
STA-13	21, 124, 179	Periodically review the organization's supply chain partners' IT governance policies and procedures.
STA-14	21, 122, 124, 179	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.
Threat and Vulnerability Management		

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
TVM-01	51	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.
TVM-02	22, 23, 24, 183	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.
TVM-03	34, 35, 45, 46, 51, 60	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.
TVM-04	51, 183	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.
TVM-05	24, 36, 51	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.
TVM-06	21, 56	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.
TVM-08	51	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.
TVM-09	51	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.
TVM-10	51	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.
Universal Endpoint Management		
UEM-01	22, 23, 24, 109, 136, 184	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.

CSA Star Criteria to Controls Mapping

CSA Star

Criteria	Controls List	Criteria
UEM-02	73, 76, 136, 184	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.
UEM-03	36, 184	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.
UEM-04	180	Maintain an inventory of all endpoints used to store and access company data.
UEM-05	22, 23, 136, 184	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.
UEM-06	185	Configure all relevant interactive-use endpoints to require an automatic lock screen.
UEM-07	34, 45, 46	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.
UEM-08	136, 184	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.
UEM-09	183	Configure managed endpoints with anti-malware detection and prevention technology and services.
UEM-10	91, 126, 158, 159, 184	Configure managed endpoints with properly configured software firewalls.
UEM-11	27, 66, 158, 186, 187, 188	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.
UEM-12	136, 184	Enable remote geo-location capabilities for all managed mobile endpoints.
UEM-13	125, 136, 184	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.

SECTION V - Other Information Provided by Google LLC

Other Information Provided by Google LLC

Internal Google Traffic

Connections between internal Google resources use proprietary services similar to Remote Procedural Calls (RPC) that provide peer-to-peer authentication similar to Kerberos. All traffic is at least cryptographically authenticated between machines, while some connections, including to and from the Key Management Service, are encrypted using AES.

Key Management

Google uses a proprietary service to manage the distribution, generation and rotation of cryptographic keys. Files or data structures with user-generated content written by Cloud or App Engine services are encrypted with a key. This key is encrypted by the Key Management Service with a restricted access control list (ACL) of services allowed to request the Key Management Service to decrypt it. The encrypted key is not stored alongside the encrypted data.

The wrapping keys needed to decrypt user data are only known to the Key Management Service. All access to/from the Key Management Service is controlled by ACLs. Access is restricted to a limited number of individuals and applications, and auditing is enabled to determine whether access is appropriate.

Key Rotations

Google uses a proprietary system to periodically generate and rotate an encryption key used to protect user data at rest on average at least every 90 days. New wrapped encryption keys are generated for each new Google storage file (a Google file is defined in Encryption of Data Stored at Google above). The system helps ensure that key rotations are managed appropriately, and that customer data is not encrypted with a discarded key.

Disk Erase Process

Google has a policy stating that no loose drive may leave Google data centers unless it has been erased (or destroyed), certified as erased by Google, and validated as such by Google via audit. One or more types of disk erase mechanisms are used to delete data off disks before they are decommissioned. Multiple checks are performed to help ensure that all drives are accounted for. Non-erased loose drives are stored in a secure container until they are erased. The disk erase process is well defined, and each facility is audited on a daily basis to monitor compliance with the disk erase policy.

If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.