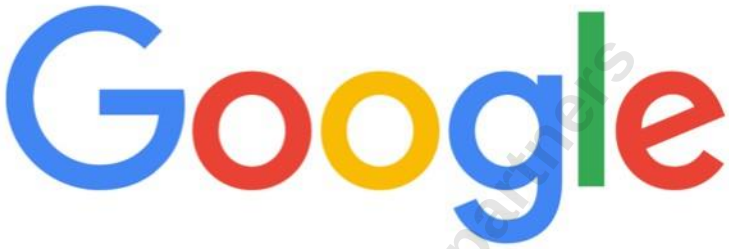

System and Organization Controls (SOC) 2 Type II Report

Description of the Google Workspace, Application Programming Interfaces and Developer Offerings System

For the Period 1 May 2022 to 30 April 2023

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 of the Google Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings System (System) that may be useful when assessing the risks arising from interactions with the System throughout the period 1 May 2022 to 30 April 2023, 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 for security, availability, confidentiality, and privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Complementary user entity controls: The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Google's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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 2022 to 30 April 2023 in accordance with the Description Criteria
(b) The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls assumed in the design of Google's controls throughout the period 1 May 2022 to 30 April 2023
(c) The Google controls stated in the Description operated effectively throughout the period 1 May 2022 to 30 April 2023 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls assumed in the design of Google's controls throughout the period 1 May 2022 to 30 April 2023

Google LLC
14 June 2023

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 of the Google Workspace, Application Programming Interfaces and Developer Offerings System" for the communication, productivity, collaboration, and security services provided to user entities throughout the period 1 May 2022 to 30 April 2023 (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 included in the Description throughout the period 1 May 2022 to 30 April 2023 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security, availability, confidentiality, and privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Complementary user entity controls: The Description also 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 extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

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 the 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 the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on

Building a better working world

the applicable trust services criteria. Google is responsible for (1) selecting the trust services criteria applicable to the Description; (2) preparing the Description and Assertion; (3) the completeness, accuracy, and method of presentation of the Description and Assertion; (4) providing the services covered by the Description; (5) identifying the risks that would 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 described 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 described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Performing procedures to obtain evidence about whether the controls stated in the Description are 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
- 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
- Testing the operating effectiveness of those controls based on the applicable trust services criteria

- Evaluating the overall presentation of the Description

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

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 users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

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

Description of tests of controls

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

Opinion

In our opinion, in all material respects:

(a) The Description presents the Google Workspace, Application Programming Interfaces and Developer Offerings System that was designed and implemented throughout the period 1 May 2022 to 30 April 2023 in accordance with the Description Criteria

(b) The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if user entities applied the controls assumed in the design of Google's controls throughout the period 1 May 2022 to 30 April 2023

(c) The controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the

Building a better working world

applicable trust services criteria throughout the period 1 May 2022 to 30 April 2023, if the user entity controls assumed in the design of Google's controls operated effectively throughout the period 1 May 2022 to 30 April 2023

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 Workspace, Application Programming Interfaces and Developer Offerings System during some or all of the period 1 May 2022 to 30 April 2023 and prospective user entities, independent auditors and practitioners providing services to such user entities 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, including complementary user entity controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

Ernst & Young LLP

14 June 2023
San Jose, CA

SECTION III - Description of the Google Workspace, Application Programming Interfaces and Developer Offerings System

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Description of the Google Workspace, Application Programming Interfaces and Developer Offerings 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's product offerings, including Google Workspace, Application Programming Interfaces and Developer Offerings (Google Workspace Services), 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 Workspace, Application Programming Interfaces and Developer Offerings are targeted to small and medium businesses and large corporations alike. These products provide what business organizations typically require, including the following:

- Multi-user collaboration
- No special hardware or software required by the enterprise
- Security and compliance features
- Seamless upgrades

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

Google Workspace Editions / SKUs

The Google Workspace brand is reflected in the related agreements and supporting documentation made available by Google.

G Suite Basic

- "G Suite Basic" is an edition of Google Workspace composed of all of the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, Google Workspace Migrate, and Workspace Add-ons.

"Workspace Add-Ons" are, collectively, Google SIP Link, Google Voice, Google Workspace Assured Controls, Workspace Additional Storage, and Meet Global Dialing.

G Suite Business

- "G Suite Business" is an edition of Google Workspace composed of all of the Google Workspace Services except Client-Side Encryption and Workspace Add-Ons. G Suite Business also includes data region policy settings for primary data within Customer Data for certain Services.

Google Workspace Business Starter

- "Google Workspace Business Starter" is an edition of Google Workspace composed of all of the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, Google Workspace Migrate, and Workspace Add-Ons. Google Workspace Business Starter Customers are limited to a maximum of 300 End Users.

Google Workspace Business Standard

- "Google Workspace Business Standard" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, and Workspace Add-Ons. Google Workspace Business Standard Customers are limited to a maximum of 300 end users.

Google Workspace Business Plus

- "Google Workspace Business Plus" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Cloud Search, and Workspace Add-Ons. Google Workspace Business Plus Customers are limited to a maximum of 300 end users.

Google Workspace Enterprise Starter

- "Google Workspace Enterprise Starter" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, and Workspace Add-Ons.

Google Workspace Enterprise Standard

- "Google Workspace Enterprise Standard" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Cloud Search, and Workspace Add-Ons. Google Workspace Enterprise Standard also includes data loss prevention functionality for Gmail and Google Drive, and certain enhanced security and control features for administrators (not including Google Workspace Security Center). Google Workspace Enterprise Standard will also allow for additional Gmail integration with other Google products, certain third-party archiving tools, and third-party OAuth applications.

Google Workspace Enterprise Plus

- "Google Workspace Enterprise Plus" is an edition of Google Workspace composed of all the Google Workspace Services except Workspace Add-Ons. Google Workspace Enterprise Plus also includes data loss prevention functionality for Gmail and Google Drive, data region policy settings for primary data within customer data for certain services, additional search and assist capabilities for content within third-party data sources (which are only available to customers with at least 500 End User licenses), and enhanced security and control features for administrators (including Google Workspace Security Center). Google Workspace Enterprise Plus will also allow for additional Gmail integration with other Google products, certain third-party archiving tools, and third-party OAuth applications.

Google Workspace for Education

- “Google Workspace for Education Fundamentals” is a free edition of Google Workspace composed of the Google Workspace Services except Client-Side Encryption, Currents, Google Cloud Search, Google Workspace Migrate, and Workspace Add-Ons. This edition also includes Assignments, Classroom and Chrome Sync as Core Services.
- "Google Workspace for Education Standard" is an upgrade to Google Workspace for Education Fundamentals that is available at an additional cost. It includes additional features such as data region policy settings for primary data within customer data for certain services, advanced security controls, enhanced analytics, and Google Workspace Migrate.
- "Google Workspace for Education Teaching and Learning Upgrade" is an upgrade to Google Workspace for Education Fundamentals that is available at an additional cost. It includes additional features for communication, collaboration, class management, and additional storage equal to 100GBs times the number of end user licenses.
- “Google Workspace for Education Plus” is an upgrade to Google Workspace for Education Fundamentals that is available at an additional cost. It includes additional features such as data region policy settings for primary data within customer data for certain services, advanced controls, enhanced analytics and search (but search and assist capabilities for content within third party data sources are only available to customers with at least 500 End User licenses), Google Workspace Migrate, and additional features for communication, collaboration, class management, and additional storage equal to 20GBs times the number of end user licenses.

Google Workspace Archived User

- The “Archived User” offering for each Google Workspace or G Suite edition allows an organization to maintain End User Accounts for former End Users for Customer’s data archival purposes. The following editions of Google Workspace Archived User include Google Vault:
    - G Suite Business - Archived User
    - Google Workspace Business Plus - Archived User
    - Google Workspace Enterprise Standard - Archived User
    - Google Workspace Enterprise Plus - Archived User

Google Workspace Essentials Starter

- "Google Workspace Essentials Starter" is a free edition of Google Workspace comprised of the services within the “Google Workspace Essentials” edition, but with different storage capacities. Customers will have a limit of 100 total end users licenses.

Google Workspace Essentials

- "Google Workspace Essentials" is an edition of Google Workspace composed of Google Calendar, Google Chat, Google Docs, Google Drive, Google Forms, Google Jamboard, Google Keep, Google Meet, Google Sheets, Google Sites, Google Slides, and Google Tasks and the following as used in conjunction with the foregoing Services: (a) Cloud Identity Management, (b) Google Contacts, and (c) Google Groups for Business.

Google Workspace Enterprise Essentials

- "Google Workspace Enterprise Essentials" is an edition of Google Workspace composed of the services within the "Google Workspace Essentials" edition, but with different storage capabilities.

Google Workspace Enterprise Essentials Plus

- "Google Workspace Enterprise Essentials Plus" is an edition of Google Workspace composed of the services within the "Google Workspace Essentials" edition, but with the following features: (a) Google Workspace Enterprise Essentials Plus also includes data loss prevention functionality for Google Drive, data region policy settings for primary data within customer data for certain services, and certain enhanced security and control features for administrators (including Google Workspace Security Center); and (b) different storage capabilities.

Google Workspace Frontline

- "Google Workspace Frontline Starter" is an edition of Google Workspace composed of all the Google Workspace Services except Client-Side Encryption, Google Vault, Google Cloud Search, Google Workspace Migrate, and the Workspace Add-Ons.
- "Google Workspace Frontline Standard" is an edition of Google Workspace composed of all the Google Workspace Services except Google Cloud Search, Google Workspace Migrate, and the Workspace Add-Ons. Google Workspace Frontline Standard also includes data loss prevention functionality for Gmail and Google Drive, and certain enhanced security and control features for Administrators (not including Google Workspace Security Center).

Google Workspace for Nonprofits

- "Google Workspace for Nonprofits" is a free edition of Google Workspace composed of the Google Workspace Services except Client-Side Encryption, Currents, Google Cloud Search, Google Workspace Migrate, and the Workspace Add-Ons. This edition also includes Classroom (as defined in “Google Workspace for Education Fundamentals” above) as a Core Service.

Cloud Search Platform

- "Cloud Search Platform" is an edition of Google Workspace composed of Google Cloud Search and the following services for use in conjunction with Google Cloud Search: (a) Cloud Identity Management; (b) Google Contacts; and (c) Google Groups for Business. Cloud Search Platform provides search and assist capabilities for content within third-party data sources.

Google Workspace Add-ons

Google Voice and Google SIP Link

- "Voice Starter" is a version of Google Voice that can be added at an additional cost to any edition of Google Workspace and that allows only up to 10 end users in a single country.
- "Voice Standard" is a version of Google Voice that can be added at an additional cost to any edition of Google Workspace and that supports any number of end users in a single country. Voice Standard also includes Google SIP Link, deskphone compatibility, and multi-level auto-attendant features.
- "Voice Premier" is a version of Google Voice that can be added at an additional cost to any edition of Google Workspace that supports any number of end users in multiple countries. Voice Premier also includes Google SIP Link, deskphone compatibility, multi-level auto-attendant features, and advanced reporting functionality.
- "Google SIP Link Standard" is a version of Google SIP Link that can be added at an additional cost to any edition of Google Workspace and that supports any number of end users in a single country. Google SIP Link Standard also includes deskphone compatibility and multi-level auto-attendant features.
- "Google SIP Link Premier" is a version of Google SIP Link that can be added at an additional cost to any edition of Google Workspace and that supports any number of end users in multiple countries. Google SIP Link Premier also includes deskphone compatibility, multi-level auto-attendant features, and advanced reporting functionality.

Google Workspace Assured Controls

- "Google Workspace Assured Controls" is a separate SKU that can be added at an additional cost to the Google Workspace Enterprise Plus edition. Google Workspace Assured Controls allows customers to geographically limit Google support actions related to their customer data.

Meet Global Dialing

- "Meet Global Dialing" is a separate SKU that can be added to any Google Workspace edition and that supports expanded dial-in and dial-out calling in Google Meet video meetings. There is no cost to subscribe to Meet Global Dialing, but usage is charged per minute.

Workspace Additional Storage

- "Workspace Additional Storage" is a separate SKU that can be added at an additional cost to any edition of Google Workspace as long as that edition does not limit storage on a per-End User basis. Customers may increase their total amount of pooled storage available by

10TB for each Workspace Additional Storage subscription purchased. There is no limit to the number of Workspace Additional Storage subscriptions that may be purchased.

The Google Workspace, Application Programming Interfaces and Developer Offerings (Google Workspace Services) covered in this system description consist of the following:

Google Workspace Core Services

Google Workspace Core Services are a set of applications, including Gmail, Docs, Sheets, Slides, Sites, and more, as well as a set of messaging, collaboration and security tools for organizations.

Admin Console

Google Admin Console is a management tool for Google Workspace administrators. It allows administrators to maintain all their Google Workspace services from one console. With the Google Admin Console, administrators can configure settings for Google Workspace, monitor the usage of their domains, and create user accounts.

Assignments

Assignments is an application for learning management systems that allows customer end users to distribute, collect, and grade student work.

Classroom

Classroom is a web-based service that allows customer end users to create and participate in classroom groups. Using Classroom, students can view assignments, submit homework, and receive grades from teachers.

Cloud Identity

Cloud Identity is an Identity as a Service (IDaaS) and enterprise mobility management (EMM) product. It offers the identity services and endpoint administration that are available in Google Workspace as a stand-alone product.

Cloud Search

Cloud Search is a web-based service that provides customer end users with search and assist capabilities for content within certain Google Workspace Core Services and selected third-party data sources. Google Cloud Search also provides end users with actionable information and recommendations.

Currents

Currents is a web-based service that allows customer end users to share links, videos, pictures, and other content with others within the same Google Workspace domain, and to view and interact with content shared with them by others within that same domain. Customer end users can also create and join communities to have conversations with others within the same domain who share their interests.

Gmail

Gmail is a web-based e-mail service that allows an organization to run its e-mail system using Google's systems. It provides the capability to access an end user's inbox from a supported web browser, read mail, compose, reply to, and forward mail, search mail, and manage mail through labels. It provides filtering for spam and viruses and allows administrators to create rules for handling messages containing specific content and file attachments or routing messages to other mail servers.

Google Calendar

Calendar is a web-based service for managing personal, corporate/organizational, and team calendars. It provides an interface for customer end users to view their calendars, schedule meetings with other end users, see availability information of other end users, and schedule rooms and resources.

Google Chat

Chat is a web-based service that allows for real time communication between customer end users. The service provides an enhanced chat messaging and group collaboration platform that allows content integrations with select third-party services.

Google Contacts

Contacts is a web-based service that allows customer end users to import, store, and view contact information, and create personal groups of contacts that can be used to email many people at once.

Google Docs

Docs is a web-based service that enables customer end users to create, edit, share, collaborate, draw, export, and embed content on documents.

Google Drive

Drive provides web-based tools enabling customer end users to create, store, transfer, and share files, and view videos.

Google Forms

Forms is a web-based service that enables customer end users to create, edit, share, collaborate, export, and embed content in forms.

Google Groups for Business

Groups is a web-based service that allows customer end users and website owners to create and manage collaborative groups to facilitate discussions and content sharing.

Google Hangouts

Hangouts is a web-based service that allows for real time communication between customer end users. The service provides one-on-one and group conversations via chat messaging, and voice, as well as lightweight video meetings.

Google Jamboard

Jamboard is a web-based service that allows customer end users to create, edit, share, collaborate, draw, export, and embed content within a document.

Google Keep

Keep is a web-based service that enables customer end users to create, edit, share, and collaborate on notes, lists, and drawings.

Google Meet

Meet is a web-based service that allows for real time communication between customer end users. The service provides enhanced large-capacity video meetings.

Google Sheets

Sheets is a web-based service that enables customer end users to create, edit, share, collaborate, draw, export, and embed content on spreadsheets.

Google Sites

Sites allows end users to create a site through a web-based tool, and then can share the site with a group of other end users or publish the site to the entire company or the world (if permitted by the Administrator). The site owner can choose who can edit a site and who can view the site.

Google Slides

Slides is a web-based service that enables customer end users to create, edit, share, collaborate, draw, export, and embed content on presentations.

Google Tasks

Tasks is a web-based service that enables customer end users to create, edit, and manage their tasks.

Google Vault

Vault is a web-based service that provides search and export capabilities for Google Drive and Gmail. For Gmail, Google Vault provides customers with the ability to search across the entire domain, to archive data, and create retention and disposition rules based on content, and eDiscovery capabilities which allow a customer to create matters and preserve this data for legal hold purposes.

Google Voice

Google Voice is an admin-managed Internet Protocol (IP)-based telephony service. It allows customers to assign and manage phone numbers for use by end users in their organization. End users can make and receive calls using their assigned numbers; additional functionalities are also available for use in connection with inbound and outbound calling, including the dialing of emergency numbers for end users using two-way dialing.

Google Workspace Migrate

Google Workspace Migrate provides data migration solutions that enable customers to easily move their on-premises or other-cloud data into Google Workspace.

Mobile Device Management

Organizations can use Google Mobile Device Management to manage, secure, and monitor mobile devices in their organization. Administrators can manage a range of devices, including phones, tablets, and smartwatches.

* Google Hangouts was deprecated on 1 November 2022

Application Programming Interfaces (APIs) and Developer Offerings

Application Programming Interfaces (APIs) and Developer Offerings are collection of tools and resources that let customers integrate their software with Google Workspace and its users or develop new apps that run entirely within Google Workspace. The offerings included in this system description are Apps Script, Product APIs and the Admin Software Development Kits (SDK).

Apps Script

Google Apps Script is a rapid application development platform that makes it fast and easy to create business applications that integrate with Google Workspace.

Product APIs

Product APIs allow applications to integrate with Google Workspace products and other Google Workspace data.

Calendar API

Calendar API enables the creation of new events in a user's Google Calendar, editing or deleting existing events, and searching for events.

*Contacts API**

Contacts API allows client applications to view and update a user's contacts. Contacts are stored in the user's Google Account; most Google services have access to the contact list.

Drive Activity API

Drive Activity API lets a customer’s application retrieve information about a user's Google Drive activity. This API provides additional functionality on top of the existing Drive API to display activity on a user’s profile, track changes to specific files or folders, and alert a user to new comments or changes to file.

Drive Rest API

Drive Rest API allows applications to interact with nearly any aspect of a user's Google Drive, including permissions, file revisions, and connected apps.

Gmail Rest API

Gmail Rest API enables applications to read messages from Gmail, send emails, modify the labels applied to messages and threads, and search through existing mail.

People API

People API enables applications to read and manage the authenticated user's contacts, read and copy the authenticated user's "other contacts", read profile information for authenticated users and their contacts, and read domain profiles and contacts.

Sheets API

Sheets API provides comprehensive access to read, write, and format data in Google Sheets.

*Sites API***

Sites Data API allows client applications to access and modify Google Site data using Google Data API feeds.

Tasks API

Tasks API provides access to search, read, and update organization-owned Google Tasks content and metadata.

Admin SDK

Admin SDK is a collection of tools which allows developers to write applications to manage Google Workspace domains, migrate from and integrate with existing IT infrastructure, create users, update settings, audit activity, and more. Scripts and add-ons (e.g., APIs) developed by end users are out of the scope of this report.

Alert Center API

Alert Center API lets customers manage alerts affecting their domain. Domain administrators can see and manage alerts manually from the Google Admin console. The Alert Center API lets apps customers retrieve alert data and alert feedback. The API can also create new alert feedback for existing alerts.

Data Transfer API

Data Transfer API manages the transfer of data from one user to another within a domain. One use case of this transfer is to reallocate application data belonging to a user who has left the organization.

Directory API

Directory API lets customers perform administrative operations on users, groups, organizational units, and devices in the organization's account.

Domain Shared Contacts API

Domain Shared Contacts API allows client applications to retrieve and update external contacts that are shared to all users in a Google Workspace domain.

Email Audit API

Google Workspace Email Audit API allows Google Workspace administrators to audit a user's email, email drafts, and archived chats. In addition, a domain administrator can download a user's mailbox.

Enterprise License Manager API

Enterprise License Manager API allows administrators to manage license assignments for Google Workspace services used by the organization.

Groups Migration API

Groups Migration API manages the migration of shared emails from public folders and distribution lists to a group's discussion archive.

Groups Settings API

Groups Settings API allows organizations to programmatically manipulate Google group settings for their domain.

Reports API

Reports API gives administrators of Google Workspace domains (including resellers) the ability to create custom usage reports for their domain.

Reseller API

Reseller API lets reseller administrators place customer orders and manage monthly postpaid subscriptions.

SAML-based SSO API

SAML-based SSO API enables customer end users to access their enterprise cloud applications by signing in one time for all services. If a user tries to sign-in to the Admin console or another Google service when SSO is set up, they are redirected to the SSO sign-in page.

* Contacts API was replaced by People API

** Sites API was deprecated on 30 January 2023

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 Workspace, Application Programming Interfaces and Developer Offerings:

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
- Clarksville (TN), United States of America
- Columbus (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Henderson (NV), 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
- Midlothian (TX), United States of America
- Moncks Corner (SC), United States of America
- Montreal, Quebec, Canada
- New Albany (OH), United States of America
- Osasco, Brazil
- Papillion (NE), United States of America
- Pryor Creek (OK), United States of America
- Quilicura, 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
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Toronto, Ontario, Canada
- Vinhedo, Brazil
- Widows Creek (AL), United States of America

Europe, Middle East, and Africa

- Doha (1), 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
- Fredericia, Denmark
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- London (1), United Kingdom
- London (2), 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, Netherlands
- Milan (1), Italy
- Milan (2), Italy
- Paris (1), France
- Paris (2), France
- Paris (3), France
- Tel Aviv (1), Israel
- Tel Aviv (2), Israel
- Turin (1), Italy+
- Turin (2), Italy+
- Turin (3), Italy+
- Warsaw (1), Poland
- Warsaw (2), Poland
- Warsaw (3), Poland+
- Zurich, Switzerland

Asia Pacific

- Changhua, Taiwan
- Delhi (1), India
- Delhi (2), India+
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Inzai, Chiba, Japan+
- Jakarta (1), Indonesia
- Jakarta (2), Indonesia
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Lok Yang Way, Singapore
- Loyang, Singapore+
- Melbourne, Victoria, Australia
- Mumbai (1), India
- Mumbai (2), India+
- Mumbai (3), India+
- Mumbai (4), India+
- Osaka, 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 centers in scope only for the period 1 November 2022 through 30 April 2023

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 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 Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings System. Commitments to customers are communicated via Terms of Service, Google Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings Terms of Service and/or Data Processing Agreements, and complies with applicable regulations
- **Data Security:** Google maintains data security and privacy policies and implements technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Google takes appropriate steps to ensure compliance with the security measures by its employees, contractors, and vendors to the extent applicable to their scope of performance
- **Third-Party Risk Management:** Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Google conducts routine inspections of subprocessors to ensure their continued compliance with the agreed upon security and privacy requirements. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from suppliers to comply with these practices.

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 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 Workspace, Application Programming Interfaces and Developer Offerings System 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 Workspace, Application Programming Interfaces and Developer Offerings' products. These risk management and mitigation activities are so critical that they have been integrated into Google's repeatable process models.

At a corporate level, there are multiple functional areas, including Legal, Information Security, Internal Audit, Privacy Engineering, Privacy Compliance, and the Office of Compliance & Integrity, 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 Workspace, Application Programming Interfaces and Developer Offerings. 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 Workspace, Application Programming Interfaces and Developer Offerings. 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 Workspace, Application Programming Interfaces and Developer Offerings, 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 Workspace, Application Programming Interfaces and Developer Offerings 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).

As part of its Google Voice and Google Meet service offerings, Google partners with Telephony Providers (https://workspace.google.com/terms/service-terms/voice/providers.html and https://workspace.google.com/terms/service-terms/meet-telephony/providers.html) to perform outbound dialing and accept inbound calls, as applicable; and process Customer Data as independent controllers in the countries in which they are located (see section Provision of Google Telephony Services in Google Workspace Service Specific Terms). Telephony providers are not subprocessors but are subject to Google's VSA process.

Data Confidentiality and Privacy

Google has established training programs for privacy and information security to support data confidentiality and privacy. All 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 web sites exist to track and monitor progress of Google Workspace, Application Programming Interfaces and Developer Offerings 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.

Internal Functions and Policies

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

Google has communicated to employees and extended workforce instructions and mechanisms for reporting potential security and privacy concerns or incidents. Google has also implemented various methods of communication to help ensure that user entities understand Google's commitments to security, availability, confidentiality, and privacy for Google Workspace, Application Programming Interfaces and Developer Offerings; and to help ensure that significant events are communicated to user entities in a timely manner. The primary conduit for communication is the Google web site, 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

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 vendors with access to the Google environment. Google's security policies describe security objectives, provide a security framework, and emphasize the importance of security to Google's business. Security policies are reviewed at least annually. Policies, FAQs, and guidelines are updated as needed.

Information Privacy Program

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

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

Network Architecture and Management

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

Google has implemented perimeter devices to protect the Google network from external attacks. Google segregates networks based on 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. Configurations of perimeter devices are centrally managed. Current and previous versions of each router configuration are maintained. Google has documented procedures and checklists for configuring and installing new servers, routers and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet.

Google has a firewall configuration policy that defines acceptable ports that may be used on a Google firewall. Only authorized services and protocols that meet Google's requirements are permitted access to the network. The firewalls are designed to automatically deny all unauthorized packets not configured as acceptable. Administrative access to the firewalls is limited to authorized administrative personnel using the 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

Strong authentication and access controls are implemented to restrict access to Google Workspace, Application Programming Interfaces and Developer Offerings 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) 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 Workspace, Application Programming Interfaces and Developer Offerings 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 employee access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system that utilizes Secure Shell (SSH) and TLS certificates help provide secure and flexible access. These mechanisms are designed to grant access rights to systems and data only to authorized users. Additionally, access requests via "on demand request" mechanisms are reviewed and approved by a second individual prior to being granted and the event is logged.

Both user and internal access to customer data are restricted through the use of unique user account IDs and via the Google Accounts Bring Your Own Identity (BYOID) system externally. Access to sensitive systems and applications requires two-factor authentication in the form of unique user IDs, strong passwords, security keys, and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data (and other need-to-know data) is appropriate and authorized. Access to production machines, network devices and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semiannual basis under the direction of the group administrators to ensure that access has been removed for employees who no longer have a business need for such access.

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

Password Guidelines

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

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

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

Google has supplemented passwords with a two-factor authentication requirement for internal personnel to access sensitive internal corporate and production services and to access Google Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings 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 (e.g. Google-Owned and Third-Party Owned) for physical security to help protect production servers, network devices, and network connections within Google data centers. Guidelines for evaluating the security of data centers are described in Google's data center security evaluation criteria. Additionally, data center personnel perform periodic surveys and reviews of data centers. Data centers that house Google Workspace, Application Programming Interfaces and Developer Offerings systems and infrastructure components are reviewed 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. Only authorized Google employees or contractors permanently working at the data centers are permitted to request standing access to the facility areas needed for their role and responsibilities. Data center access requests must be made through internal tools and require the approval of authorized data center personnel. All other Google employees and authorized contractors requiring temporary data center access must also have an approved access request and register at the guard station upon arrival. User access lists to data center server areas are reviewed 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, 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 Workspace, Application Programming Interfaces and Developer Offerings are delivered as software releases. Change Management policies, 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.

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 that code changes follows Google coding standards.

Once the code is merged, it can be used to build software binaries. During the build process, code is subject to automated testing, the results of which are monitored by engineers. Successfully built binaries can be migrated to staging or QA environments where they can be subject to additional review. When software is ready for deployment to production, it is deployed in a controlled manner, with monitoring in place to notify engineers of anomalies in the deployment. The process from build to release is aided by several tools that automate tasks, including testing and deployment. Employees at Google have the ability to view changes, however, access to modify code and approve changes is controlled via functionality of internal tools that supports 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 Workspace, Application Programming Interfaces and Developer Offerings 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

Log sources are used to generate alerts whenever an anomaly occurs. Production monitoring tools, in response to an anomaly, automatically generate alerts to relevant teams based on the anomaly configurations set by each team. An anomaly may also be manually documented by a Google employee when an issue is identified or in response to a customer service request.

Production systems are configured to send system events to monitoring and alerting tools. Google personnel use these tools to respond to potential incidents, including security and privacy incidents.

Alerts capture 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 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 Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Structured data is then stored in large, distributed databases, built on top of this file system.

The data centers are connected through multiple encrypted network links and interfaces. 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.

Data within Google Workspace Core Services are periodically backed up to support the availability of user entity data. Google Workspace Core Services data restore tests are periodically performed on a subset of data to confirm the availability to recover customer data from backups.

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.

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 Workspace, Application Programming Interfaces and Developer Offerings.

Security Monitoring

Google has implemented monitoring tools to detect and report security events. Antivirus, phishing detection, and antimalware/antispam tools are also in place to protect Google's information assets. Google also maintains security event logs for privileged access, access to user data, authorized access attempts, and unauthorized access attempts. Logical access to security event logs is restricted to authorized personnel. Security event logs are monitored continuously using a Google proprietary Security Event Management (SEM) system to detect intrusion attempts and other security related events. The SEM is supplemented with codified logic which creates the “hunts” that trigger automated alerts to security personnel. The security alerts are generated for further investigation (manual and automated hunts) based on predefined thresholds. When a vulnerability has been identified, the Security team determines the appropriate response and tracks the issue through 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 Workspace, Application Programming Interfaces and Developer Offerings 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 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.	Customers are responsible for assigning responsibilities for the operation and monitoring of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
Common Criteria 1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Customers are responsible for providing the appropriate training to end-users on proper use of the Google Workspace, Application Programming Interfaces and Developer Offerings System consistent with the Acceptable Use Policies and Terms of Service. Acceptable Use Policies available at (or such URL as Google may provide): • Google Workspace: https://workspace.google.com/terms/use_policy.html

Trust Services Criteria	Complementary User Entity Controls (CUECs)
	Customers are responsible for ensuring that end-users are trained on the organizational policies and procedures relevant to the use of the Google Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for training users on the use and disclosure of passwords used to authenticate to the Google Workspace, Application Programming Interfaces and Developer Offerings System.
Common Criteria 1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. Common Criteria 5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
Common Criteria 2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. Common Criteria 2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Customers are responsible for defining, documenting, and making available to users procedures for the operation of their instance of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for identifying and managing the inventory of information assets on the Google Workspace, Application Programming Interfaces and Developer Offerings 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.	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	Customers are responsible for ensuring any application software which they deploy onto the Google Workspace, Application Programming Interfaces and Developer Offerings System follows their specific software change management policies and procedures.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
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 Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings 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 Workspace, Application Programming Interfaces and Developer Offerings 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.

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

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Customers are responsible for provisioning service availability, user roles, and sharing permissions within the Google Workspace, Application Programming Interfaces and Developer Offerings System consistent with customer organizational policies.
	Customers are responsible for implementing secure log-on procedures to access the Google Workspace, Application Programming Interfaces and Developer Offerings 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.
	Customers are responsible for establishing procedures to allocate the initial password to access the Google Workspace, Application Programming Interfaces and Developer Offerings System to end-users when Google password authentication is used.
	Google Workspace Marketplace offers enterprise applications that can be added to a Google Workspace domain to enhance functionality and features to native Google applications. Customers are responsible for configuring third party Marketplace apps permissions in the Google Workspace Services consistent with their policies.
	Customers are responsible for restricting access to and monitoring the use of Application Programming Interfaces (APIs) available in the Google Workspace, Application Programming Interfaces and Developer Offerings System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
	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 Workspace, Application Programming Interfaces and Developer Offerings 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.	Customers are responsible for ensuring appropriate physical security controls over all devices that access the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for ensuring any devices that access the Google Workspace, Application Programming Interfaces and Developer Offerings System or contain customer data are properly handled, secured, and transported as defined by the products requirements.
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Customers are responsible for configuring the Google Workspace, Application Programming Interfaces and Developer Offerings System mobile device options consistent with customer policies and procedures.

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. Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Customers are responsible for enabling logging and monitoring functionalities to detect administrator activity, customer support activity, security events, system errors, and data deletions to support customer incident management processes.
Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. Privacy Criteria 7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	Customers are responsible for considering information security requirements in the deployment, configuration, and modification of their instance of the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of the Google Workspace, Application Programming Interfaces and Developer Offerings System.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Customers are responsible for ensuring that individuals creating and/or updating profiles or changing the product configurations are authorized.
	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 Workspace, Application Programming Interfaces and Developer Offerings System, as applicable, and restricting access to data in these environments.
Common Criteria 9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. Common Criteria 9.2: The entity assesses and manages risks associated with vendors and business partners.	Customers are responsible for ensuring they have business recovery and backup procedures over their non-Google managed information systems that access the Google Workspace, Application Programming Interfaces and Developer Offerings System.
	Customers are responsible for developing and maintaining disaster recovery and business continuity plans for their non-Google managed business systems.

Trust Services Criteria	Complementary User Entity Controls (CUECs)
Confidentiality Criteria 1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. Privacy Criteria 4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. Privacy Criteria 5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	Customers are responsible for ensuring that administrators do not send unnecessary employee personal data when escalating support requests to service providers, including Google.

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 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 semiannually 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	Tests Performed by EY	Results
1. The organization has implemented a formal reporting structure that is made available to personnel.	CC1.3, CC1.4	Inquired of the Program Manager and determined the organization implemented a formal reporting structure that was made available to personnel.	No deviations noted.
		Inspected the organization's intranet and determined organizational charts showing formal reporting structure were made accessible to employees and included drill-down functionality to identify employees within the organizational structure, including employees in their functional teams.	No deviations noted.
		Inspected a sample communication and determined top level management changes were communicated internally and externally.	No deviations noted.
		Inspected the meeting minutes of a sample Board of Directors forum and determined management considered requirements such as integrity and security when defining authorities, structures, reporting lines, and responsibilities.	No deviations noted.
		Inspected procedural documents and determined management planned and prepared for succession by developing contingency plans for assignments of responsibility.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
2. Company goals and responsibilities are required to be developed and communicated by management on a periodic basis, and amended as needed. Results are evaluated and communicated to employees.	CC1.3, CC1.5, CC2.2, CC3.1	Inquired of the Program Manager and determined company goals and responsibilities were developed and communicated by management every quarter and amended as needed. Results of previous quarter goals were evaluated and communicated to employees every quarter.	No deviations noted.
		Inspected a sample of quarterly goals and responsibilities and determined they were developed and evaluated by management.	No deviations noted.
		Inspected a sample of quarterly announcements and determined results of previous quarter goals were communicated to employees.	No deviations noted.
3. All board of directors exercise independent judgment, while the independent / non-employee board of directors also demonstrate independence from management in exercising oversight of the development and	CC1.2, CC1.5	Inquired of the Program Manager and determined the board of directors demonstrated independence from management and had established an audit and compliance committee to exercise oversight of the development and performance of internal control.	No deviations noted.
		Inspected the Alphabet proxy statement and determined that the board of directors, including the members of the audit and compliance committee, demonstrated independence from management.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
performance of internal control.		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.
4. Information security is managed by an executive who is dedicated to Security, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.	CC1.5	Inquired of the Program Manager and determined information security 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 meeting invites 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
5. The organization has established a Code of Conduct that is reviewed and updated as needed.	CC1.1, CC9.2, C1.1	Inquired of the Program Manager and determined the Code of Conduct for employees and third parties were in place and reviewed and updated as needed.	No deviations noted.
		Inspected the Code of Conduct and determined it was reviewed and updated as needed by the organization.	No deviations noted.
6. The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	CC1.1, CC1.5	Inquired of the Program Manager and determined the organization established a disciplinary process to address non-compliance with company policies, code of conduct, or other personnel requirements.	No deviations noted.
		Inspected internal documentation and determined the organization established a disciplinary process for non-compliance with the company policies, code of conduct, or other personnel requirements which could result in dismissal, lawsuits and/or criminal prosecution.	No deviations noted.
		Inspected the disciplinary procedures undertaken for sample incidents and determined appropriate action was taken in cases of non-compliance with company policies, code of conduct, or other personnel requirements.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
7. 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	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.
8. The organization has established an offboarding procedure for personnel, which governs the removal of access and return of assets.	CC5.2	Inquired of the Program Manager and determined the organization had established offboarding procedures for personnel, which governed the removal of access and return of assets.	No deviations noted.
		Inspected internal guidelines and determined the organization had established offboarding procedures for personnel, which governed the removal of access and return of assets.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 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.
9. Personnel of the organization are required to acknowledge the Code of Conduct.	CC1.1	Inquired of the Program Manager and determined employees and extended workforce personnel were required to acknowledge the Code of Conduct as part of the terms and conditions of employment.	No deviations noted.
		Inspected internal documentation and determined employees and extended workforce personnel were required to acknowledge the Code of Conduct as part of the terms and conditions of employment.	No deviations noted.
		Inspected a sample of newly hired employees and extended workforce personnel and determined the Code of Conduct was acknowledged as part of the terms and conditions of their employment.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
10. New hires or internal transfers are required to go through an official recruiting process during which they are screened against detailed job descriptions and interviewed to assess competence.	CC1.3, CC1.4	Inquired of the Program Manager and determined 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.
		Inquired of the Program Manager and determined positions had detailed job descriptions that listed qualifications, such as requisite skills and experiences, which candidates must have met to have been hired.	No deviations noted.
		Inspected a sample of new hires and internal transfers and determined they went through a formal recruiting process and were screened against detailed job descriptions.	No deviations noted.
11. Background checks are performed on new hires as permitted by local laws.	CC1.1, CC1.4	Inquired of the Program Manager and determined background checks were performed for new hires as permitted by local laws.	No deviations noted.
		Inspected internal guidelines and determined background checks were part of the hiring process.	No deviations noted.
		Inspected a sample of new hires and determined background checks were performed as permitted by local laws.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
12. The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	CC9.2, C1.1	Inquired of the Program Manager and determined the organization required its extended workforce personnel to sign confidentiality agreements that defined responsibilities and expected behavior for the protection of information.	No deviations noted.
		Inspected the confidentiality agreements and determined the organization defined extended workforce personnel responsibilities and expected behavior for the protection of information.	No deviations noted.
		Inspected a sample of extended workforce personnel hiring records and determined the individual signed the confidentiality agreements as part of their service conditions.	No deviations noted.
13. The organization has established confidentiality agreements that are reviewed and updated as needed.	CC9.2, C1.1	Inquired of the Program Manager and determined confidentiality agreements (Google NDA, Confidential Information and Invention Assignment Agreement (CIIAA), and the Code of Conduct) for employees and third parties were in place, reviewed and updated as needed.	No deviations noted.
		Inspected the confidentiality agreements and determined they were reviewed and updated as needed by the organization.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
14. The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, CC7.2, A1.3	Inquired of the Program Manager and determined the organization conducted periodic information security risk assessments to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No deviations noted.
		Inspected the risk management guidelines 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 applicable documentation 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.
15. The organization develops and maintains a risk management framework to manage	CC3.1, CC3.2, CC3.3, CC3.4,	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	Tests Performed by EY	Results
risk to an acceptable level.	CC5.1, CC5.2	Inspected the vulnerability management and priority 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 management signed off on the risk management framework.	No deviations noted.
		Inspected the organization's risk assessment and determined the organization evaluates qualitative and quantitative factors to identify residual risk in order to manage risk to an acceptable level.	No deviations noted.
		Inspected meeting invites and relevant documentation from the organization's annual risk assessment discussion and determined the organization's operational objectives, potential impacts, and changes to the business model were considered.	No deviations noted.
		Inspected the internal insider risk site and determined the organization considered insider risk in its risk management framework to manage risk to an acceptable level.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
16. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by management.	CC3.1, CC3.2, CC3.3, CC3.4	Inquired of the Program Manager and determined the organization conducted periodic information security risk assessments to identify, evaluate, and mitigate risks to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No deviations noted.
		Inspected the risk management guidelines 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 applicable documentation 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.
17. The organization reviews and validates the design, operation and control record of in-scope compliance controls on a periodic basis.	CC4.1, CC4.2	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected evaluations performed by the internal compliance function for a sample of semiannual periods and determined the compliance function performed an evaluation of management's compliance with security, identity, authentication, and source code management controls.	No deviations noted.
		Inspected evaluations performed by management for a sample of quarters and determined management performed an evaluation of their compliance with security, identity, authentication, and source code management controls.	No deviations noted.
		Inspected the meeting invites related to Google's annual organizational risk assessment and determined the operational objectives, potential impacts and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.
18. 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	CC5.1, CC5.2	Inquired of the Program Manager and determined the organization had an internal audit function and regularly engaged independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.		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.
		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.
19. The organization has an established Internal Audit function which evaluates management's compliance with security controls.	CC4.1, CC4.2, CC5.3	Inquired of the Program Managers and Internal Audit and determined 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	Tests Performed by EY	Results
		Inspected evaluations performed by the internal compliance function for a sample of semiannual periods and determined the compliance function performed an evaluation of management's compliance with security, identity, authentication, and source code management controls.	No deviations noted.
		Inspected evaluations performed by management for a sample of quarters and determined management performed an evaluation of their compliance with security, identity, authentication, and source code management controls.	No deviations noted.
		Inspected the meeting invites related to Google's annual organizational risk assessment and determined the operational objectives, potential impacts and changes to the organization's business model were considered across various areas related to information security.	No deviations noted.
20. The organization requires external parties (Service Providers) to meet security and privacy requirements for safeguarding user data. Requirements are enforced via the	CC9.1	Inquired of the Program Manager and determined the organization required external parties (Service Providers) to meet security and privacy requirements for safeguarding user data and the requirements were enforced via the “Information Protection Addendum (IPA)” or “Partner Information Protection Addendum (PIPA)” for providers and partners, respectively.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
"Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.		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.
21. 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	CC9.2, C1.1, P6.1, P6.4, P6.5, P6.6	Inquired of the Program Manager and determined the organization required subprocessors to meet security and privacy requirements for safeguarding user data and the requirements were enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements.	No deviations noted.
		Observed the latest addendum template and determined it had defined the security and privacy obligations that subprocessors must meet to satisfy the organization's obligation regarding customer data.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
contractual agreements or other data processing terms.		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 a sample of addendum confirming that appropriate exception handling procedures for service or product issues related to vendors are in place.	No deviations noted.
22. The Security Engineering Org 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	Inquired of the Program Manager 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. Reviews included 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
23. Cloud subprocessor security and privacy risk is assessed via periodic assessment of sub-processor control environment.	CC9.2, P6.1, P6.4	Inquired of the Program Manager and determined Cloud subprocessor security and privacy risk was assessed via periodic assessment of subprocessor control environment.	No deviations noted.
		Inspected documentation of a review for a sample of subprocessors and determined that assessments of their security and privacy controls were performed on a periodic basis.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
24. Subprocessor performance is regularly assessed and monitored via periodic business reviews.	CC9.2	Inquired of the Program Manager and determined subprocessor performance was regularly assessed and monitored via periodic business reviews.	No deviations noted.
		Inspected documentation for a sample of subprocessors and determined that subprocessor performance was regularly assessed and monitored via periodic business reviews.	**Deviation noted.** For 1 of the 5 samples selected, there was no formalized Quarterly Business Review (QBR) to assess subprocessor performance. Management currently monitors only certain subprocessors.
Management's Response: Management acknowledges that there was no formalized business review to assess the performance of one sampled subprocessor. Management retroactively performed a business review for the identified subprocessor and deemed that performance was satisfactory. EY inspected documentation for the retroactively performed Quarterly Business Review for the affected sample and determined that the review was performed accordingly. Additionally, a security and privacy review had been conducted for the selected subprocessor, reducing the overall risk of this deviation. Management has reiterated the importance of subprocessor performance assessments to relevant teams to ensure that these reviews are periodically conducted in the future.			
25. The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and	CC9.2, C1.1	Inquired of the Program Manager and determined the organization had established agreements, including non-disclosure agreements, for preserving confidentiality of information and software exchanges with external parties, such as third-party vendors.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
software exchanges with external parties.		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.
26. The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	P1.1, P2.1, P4.2, P4.3	Inquired of the Program Manager and determined the organization maintained policies regarding the return, transfer, and disposal of user data and made these policies available to customers.	No deviations noted.
		Inspected publicly available documentation 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.
27. The organization only processes user data in accordance with the applicable data	P1.1, P3.1, P4.1	Inquired of the Program Manager and determined that customer data was only processed in accordance with the data processing terms and not for any other purpose.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
processing terms and does not process user data for any other purpose.		Inspected the Google Workspace Data Processing Addendum 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.
		Observed a user upload data to Google Workspace 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.
		Inquired of Product Counsel 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.
28. Customers are notified of user data requests from government agencies in accordance with the procedure agreed upon	P6.1, P6.7	Inquired the Program Manager and determined that customers were notified of data requests from government agencies in accordance with the procedure and time period agreed upon in the contract, unless such notification was otherwise prohibited.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
in the contract, unless such notification is otherwise prohibited.		Inspected the Google Workspace 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.
		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 a sample of disclosure requests and determined notification was sent to the customers in accordance with contractual requirements.	No deviations noted.
29. Where the organization is a data processor, the organization maintains and makes available a list of subprocessors and updates that list, as contractually required.	P6.1, P6.4	Inquired of the Program Manager and determined that where the organization is a data processor, the organization maintained and made available a list of subprocessors and updated that list, as contractually required.	No deviations noted.
		Inspected Google Workspace's public-facing website and determined an updated list of all subprocessors was publicly available, as contractually required.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample email notification and determined notice of subprocessor changes were sent to customers.	No deviations noted.
30. The organization provides mechanisms to notify customers in the event its confidentiality practices are discontinued, or changed to be less restrictive.	CC2.3, C1.1	Inquired of the Program Manager and determined the organization provided mechanisms to notify customers should Google's confidentiality practices be discontinued or changed to be less restrictive.	No deviations noted.
		Inspected Google's Terms of Service and determined Google provided mechanisms to notify customers should Google's confidentiality practices be discontinued or changed to be less restrictive.	No deviations noted.
		Inspected Google Workspace's Terms of Service and determined Google provided mechanisms to notify customers should Google's confidentiality practices be discontinued or changed to be less restrictive.	No deviations noted.
		Inspected Google's Privacy Policy and determined updates to the policy were communicated to the users.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
31. Descriptions of the organization's system and its boundaries are available to external parties via ongoing communications with customers or via its official blog postings.	CC2.3	Inquired of the Program Manager and determined descriptions of the organization's system and its boundaries were available to authorized external users via ongoing communications with customers or via its official blog postings.	No deviations noted.
		Inspected the organization's official blog postings and determined descriptions of the organization's system and its boundaries were communicated.	No deviations noted.
32. Customer responsibilities are described on the organization's product websites or in system documentation.	CC2.2, CC2.3	Inquired of the Program Manager and determined customer responsibilities were described on product websites or in system documentation.	No deviations noted.
		Inspected the Google Workspace website or in system documentation accessible by external customers and determined customer responsibilities were described.	No deviations noted.
33. Changes to customer facing services that may affect confidentiality, processing integrity and / or availability are communicated to relevant personnel and impacted customers.	CC2.2, CC2.3	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.
		Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
34. The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	CC2.3	Inquired of the Program Manager and determined Google published its commitments to security, availability, and confidentiality to external users via Terms of Service (ToS).	No deviations noted.
		Inspected Google Workspace's Terms of Service and product websites and determined Google's commitments to security, availability and confidentiality are published for external users.	No deviations noted.
35. The organization has guidelines specifying the security requirements for new and existing information systems.	CC5.2, CC5.3	Inquired of the Program Manager and determined 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected publicly available documentation and determined Google outlined security requirements for new information systems, or enhancements to existing information systems related to its services.	No deviations noted.
36. The organization has policies and guidelines governing the secure development lifecycle.	CC8.1	Inquired of the Program Manager and determined the organization had policies and procedures which govern the secure development lifecycle.	No deviations noted.
		Inspected internal documentation and determined the organization had policies and procedures which govern the secure development lifecycle.	No deviations noted.
37. The organization has policies and guidelines that govern third-party relationships.	CC9.2	Inquired of the Program Manager and determined the organization developed policies and procedures that govern third party relationships.	No deviations noted.
		Inspected internal documentation and determined policies and procedures were in place to govern third party relationships.	No deviations noted.
		Inspected Google Cloud third party policy and determined policies and procedures were in place to govern third party relationships for Google Cloud Products.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
38. The organization has policies and guidelines that govern access to information systems.	CC5.3	Inquired of the Program Manager and determined the organization established policies and procedures that govern access to information systems.	No deviations noted.
		Inspected the relevant documentation and determined Google established policies and procedures that govern access to information systems.	No deviations noted.
39. The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	CC2.2, CC5.3	Inquired of the Program Manager and determined the organization had security policies addressing confidentiality, integrity, and availability that were approved by management and published on the intranet which is accessible to employees.	No deviations noted.
		Inspected internal documentation and determined security policies addressing confidentiality, integrity and availability 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	Tests Performed by EY	Results
40. The organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	CC2.1, CC2.2	Inquired of the Program Manager and determined the organization established security policies and procedures, which clearly defined information security responsibilities for all employees, including the Information Security team. The organization managed operational risk by delegating decisions on risk identification and resource prioritization.	No deviations noted.
		Inspected relevant security policies and procedures and determined they defined information security responsibilities of employees and the Information Security Team.	No deviations noted.
		Inspected Google's risk assessment and determined the organization managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of Google products and services.	No deviations noted.
41. The organization has policies and guidelines that govern the acceptable use of	CC3.2, CC6.1	Inquired of the Program Manager and determined the organization established policies and procedures that governed the acceptable use of information assets.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
information assets.		Inspected the relevant documentation and determined Google established policies and procedures that governed the acceptable use of information assets.	No deviations noted.
42. The organization has a published User Data Wipeout Policy.	CC6.1, C1.1, C1.2, P4.2, P4.3	Inquired of the Program Manager and determined Google had a User Data Retention and Deletion Policy.	No deviations noted.
		Inspected the User Data Retention and Deletion Policy and other related documentation, and determined it established guidelines to govern the retention and deletion of user data.	No deviations noted.
43. The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.	CC6.4, CC6.7	Inquired of the Data Center Security Manager and determined 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.
44. The organization maintains policies that define the requirements for the use of	CC6.7	Inquired of the Program Manager and determined the organization established policies and procedures that govern the internal and external use of cryptographic controls.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
cryptography.		Inspected the security policies and procedures and determined they covered governance of the internal and external use of cryptographic controls.	No deviations noted.
		Inspected a Google Workspace relevant documentation and determined they covered governance of the internal and external use of cryptographic controls.	No deviations noted.
45. The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	CC6.7	Inquired of the Program Manager and determined the organization maintained policies for securing mobile devices used to access corporate network and systems.	No deviations noted.
		Inspected relevant policies and documentation and determined the organization maintained policies for securing mobile devices used to access corporate network and systems.	No deviations noted.
46. The organization has established policies and guidelines to govern data classification, labeling and security.	CC6.1, C1.1, P4.1	Inquired of the Program Manager and determined the organization has established policies and guidelines to govern data classification, labeling and security.	No deviations noted.
		Inspected relevant documentation and determined Google established policies and guidelines to govern data classification, labeling and security.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
47. The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	CC5.3, CC7.5	Inquired of the Program Manager and determined change management policies, including security code reviews, were in place, and procedures for tracking, testing, approving, and validating changes were documented.	No deviations noted.
		Inspected internal policies and determined practices for security code review, tracking, testing, approving, and validating changes were documented.	No deviations noted.
48. The organization has established a process to review and approve requests for policy exceptions.	CC2.1, CC2.2	Inquired of the Program Manager and determined Google has a policy exception process to ensure a formal approval and risk evaluation are performed.	No deviations noted.
		Inspected applicable policies and determined the process to request and process policy exceptions was documented.	No deviations noted.
		Inspected a sample of policy exceptions and determined they followed the process as described in the policy.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
49. The organization has established guidelines for governing the installation of software on organization-owned assets.	CC6.7, CC8.1	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
		Inspected 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Inspected the code configuration and determined access to deploy software was restricted to authorized engineers.	No deviations noted.
50. The organization prohibits the use of removable media for the	CC6.7, P4.3	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	Tests Performed by EY	Results
storage of PII and SPII 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.
51. Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	CC4.1, CC5.3	Inquired of the Program Manager and determined security policies were reviewed at least annually, and policies, procedures and guidelines were updated as needed.	No deviations noted.
		Inspected applicable policies and guidelines and determined privacy and information security were in place.	No deviations noted.
		Inspected internal documentation and determined security policies must be annually evaluated and authorized before they are implemented.	No deviations noted.
		Inspected the most recent security policy reviews and determined security policies were approved by authorized personnel or committee, reviewed at least annually, and updated as needed.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
52. The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.	CC1.1, CC1.4, CC2.2	Inquired of the Program Manager and determined that Google established a privacy and information security training program and required relevant personnel to complete this training annually.	No deviations noted.
		Inspected relevant documentation and determined that a privacy and information security training program was in place and relevant personnel were required to complete the training annually.	No deviations noted.
		Inspected a sample email notification sent to Google employees and extended workforce 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 outlined the importance of information security and maintaining user, customer and employee privacy.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the continuing education documents and determined that Google provided support on 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.
53. Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.	CC6.1	Inquired of the Program Manager and determined access to network devices was authenticated via user ID, password, security key, and/or certificate.	No deviations noted.
		Inspected the access configuration for production network devices and determined it required authentication via user ID, password, security key, and/or certificate.	No deviations noted.
		Observed a user attempt to obtain access to network devices after authenticating via user ID, password, security key, and/or certificate and determined that the user successfully obtained access.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a user attempt to obtain access to network devices without first authenticating via user ID, password, security key, and/or certificate and determined that the user failed to obtain access.	No deviations noted.
54. Wireless connections to Corp resources at organization's facilities are encrypted.	CC6.1	Inquired of the Program Manager and determined wireless connections to corporate resources at the organization's facilities were encrypted.	No deviations noted.
		Inspected internal documentation and determined wireless connections to corporate resources at the organization's facilities were encrypted.	No deviations noted.
		Inspected a remote wireless connection to corporate resources and determined that remote access to the corporate network was encrypted.	No deviations noted.
55. The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	CC7.1	Inquired of the Program Manager and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	No deviations noted.
		Inspected the internal documentation and determined the organization had dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
56. Mechanisms are in place to detect attempts, and prevent connections to the organization's network by unauthorized devices.	CC6.1, CC6.2	Inquired of the Program Manager and determined mechanisms were in place to detect attempts and prevent connections to the organization's network by unauthorized devices.	No deviations noted.
		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.
		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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a user modify their certificate and determined that access was disconnected.	No deviations noted.
57. Logical access to network devices is restricted to authorized personnel and is periodically reviewed.	CC7.1	Inquired of the Program Manager and determined that access to network devices was restricted to authorized personnel and periodically reviewed.	No deviations noted.
		Inspected the network device access management policy and determined access to network devices was restricted to authorized personnel.	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 a sample of quarterly user access reviews performed for network devices and determined the review was performed timely and by appropriate personnel.	No deviations noted.
58. The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are	CC6.1	Inquired of the Program Manager and determined networks were segregated based on the types of services, users and information systems.	No deviations noted.
		Inspected internal documentation and determined networks were designed to be logically or physically segregated.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
physically and/or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.		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.
		Inspected network diagrams and determined high-risk environments were designed to be physically and logically segregated from other networks.	No deviations noted.
59. The organization has implemented perimeter devices to protect the corporate network from external network attacks.	CC6.6	Inquired the Program Manager and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
		Inspected the policies and documents related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the configurations related to the perimeter devices and determined that the organization implemented perimeter devices to protect the corporate network from external network attacks.	No deviations noted.
60. The organization has a security guideline that requires users to lock their workstations and mobile devices when unattended. Workstations are configured to initiate a password protected screen-saver after 15 minutes of inactivity (i.e., no input from device user).	CC6.1	Inquired of the Program Manager and determined a security guideline was in place that required users to lock workstations and mobile devices when unattended.	No deviations noted.
		Inspected internal policies and determined the organization required users to lock their workstations and mobile devices when unattended.	No deviations noted.
		Inspected the idle time configurations propagated to workstations and determined they were configured to enforce password standards.	No deviations noted.
		Performed on-site inspections for a sample of offices and determined that employees followed appropriate office security practices including 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.

Criteria, Controls, Tests and Results of Tests

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

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the configuration for corporate-managed devices with privileged access and determined the organization implemented access protection, identity, and authorization management protections.	No deviations noted.
		Inspected the device settings on a corporate-managed device with privileged access and determined access protection, identity, and authorization management protections are implemented as configured.	No deviations noted.
62. The organization has implemented mechanisms to protect its information assets against malicious activity (e.g. malware, spam, phishing).	CC6.8	Inquired of the Program Manager and determined the organization has implemented mechanisms to protect its information assets against malicious activity.	No deviations noted.
		Inspected Google's internal guidelines and determined the organization has implemented mechanisms to protect its information assets against malicious activity.	No deviations noted.
		Inspected the antivirus and antimalware mechanisms and determined that the tools were in place to protect the organization's information assets.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected internal documentation and determined antivirus software in place was configured to have a function to roll-back to a previous state in case of malfunction of an anti-virus system update.	No deviations noted.
		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.	No deviations noted.
63. Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	CC6.1, CC6.6, CC6.7	Inquired of the Program Manager and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
		Inspected internal policies regarding encryption mechanisms and determined the organization used encryption to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
		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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed connection settings to the organization's external websites for a user and an administrator and determined encryption was used to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
		Inspected the server scan results and determined the organization used encryption mechanisms to protect user authentication and administrator sessions transmitted over the Internet.	No deviations noted.
64. The organization uses encryption to secure user data in transit between the organization's production facilities.	CC6.7	Inquired of the Program Manager and determined encryption was used to secure user data in transit between the organization's production facilities.	No deviations noted.
		Inspected internal documentation and determined encryption was used to secure user data in transit between the organization's production facilities.	No deviations noted.
		Inspected the encryption configuration and determined encryption was 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	Tests Performed by EY	Results
65. Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.	CC6.8	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.
		Inspected Google's security policies and determined Google had implemented rules to govern the installation of software by users.	No deviations noted.
		Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations from pre-defined OS configurations and correct them.	No deviations noted.
		Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a Software Engineer insert a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer modify a test file in the directory of a haphazardly selected production machine and determined the tool detected the test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Observed a Software Engineer delete a test file in the directory of a haphazardly selected production machine and determined the tool detected the deleted test file and corrected the production machine back to the pre-defined OS configurations.	No deviations noted.
		Inspected the code configuration and determined access to deploy software was restricted to authorized engineers.	No deviations noted.
66. Changes to network configurations are reviewed and approved	CC8.1	Inquired of the Program Manager and determined changes to network configurations were reviewed, approved, and tested prior to deployment.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
prior to deployment.		Inspected a sample of manual network configuration changes and determined they were reviewed by a separate technical resource to validate quality and accuracy.	No deviations noted.
		Inspected a sample of manual network configuration changes and determined they were tested prior to deployment.	No deviations noted.
		Inspected a sample automated change and determined it was made by an automated tool based on the pre-configured ruleset.	No deviations noted.
		Inspected a sample change made to the automated tool and determined it was reviewed by a separate technical resource to validate quality and accuracy and tested prior to deployment.	No deviations noted.
67. A standard image is utilized for the installation and maintenance of each production server.	CC8.1	Inquired of the Program Manager and determined the organization established guidelines for governing the installation of software on organization-owned assets. Further determined that a standard production image was utilized for the installation and maintenance of each production server. Deployment of software in production was restricted to authorized personnel and mechanisms were utilized to identify and correct deviations from pre-defined OS configurations.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 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	Tests Performed by EY	Results
		Observed a Software Engineer deleted 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 code configuration and determined access to deploy software was restricted to authorized engineers.	No deviations noted.
68. Only users with a valid user certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	CC6.6, CC6.7	Inquired of the Program Manager and determined only users with a valid certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.	No deviations noted.
		Inspected relevant documentation and determined mechanisms are in place to authenticate users and restrict access to production machines without a valid digital certificate.	No deviations noted.
		Inspected the configuration 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
69. The organization has an established key management process in place to support the organization's use of cryptographic techniques.	CC6.1	Inquired of the Program Manager and determined 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	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	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.
70. The organization maintains formal user registration and de-registration procedures	CC6.2, CC6.3	Inquired of the Program Manager and determined the organization maintained formal user registration and de-registration procedures for granting and revoking access.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
for granting and revoking access.		Inspected relevant documentation and determined the organization had formal procedures for granting and revoking user access to the corporate 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.
		Inspected relevant documentation and determined the organization had formal procedures for granting and revoking user access to the production network.	No deviations noted.
		Inspected system configurations and determined the system was configured to enforce approval from a group administrator prior to modifying user access to production machines, support tools, and network devices.	No deviations noted.
		Observed an attempt to modify user access to a group with the appropriate approval and determined access was granted.	No deviations noted.
		Observed an attempt to modify user access to a group without the appropriate approval and determined access was not granted.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample system generated log for access to production machines, support tools, and network devices and determined access approvals and modifications to the access lists were recorded.	No deviations noted.
		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.
71. The organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	CC6.1	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	Tests Performed by EY	Results
		Inspected the password and idle time configurations propagated to servers and determined they were configured to enforce password requirements.	No deviations noted.
		Inspected the configuration for default password and determined users were required to change their default password.	No deviations noted.
		Observed corporate endpoint devices and determined users were locked out after reasonable amount of time of inactivity.	No deviations noted.
72. The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege.	CC6.1	Inquired of the Program Manager and determined the organization had an established policy to ensure access to information resources, including data and the systems which store or process data, was authorized based on the principle of least privilege.	No deviations noted.
		Inspected internal policies and determined 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.
73. Personnel access to sensitive internal systems and applications requires two-factor	CC6.1, CC6.6	Inquired of the Program Manager and determined access to sensitive systems and applications requires two-factor authentication in the form of user ID, password, security key, and/or certificate.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
authentication in the form of a distinct user ID and password with a security key or certificate.		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 code that enforced the authentication of users prior to the granting of a certificate and determined certificates that were required for access to production machines were only generated after a user is authenticated to single sign-on using two-factor authentication.	No deviations noted.
		Observed a user attempt to gain access to a production machine with a valid user ID, password, security key, and certificate and determined access was granted.	No deviations noted.
		Observed a user attempt to gain access to a production machine without a valid certificate and determined access was not granted.	No deviations noted.
		Observed a user attempt to gain access to a production machine with valid emergency access credentials and determined access was granted.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a user attempt to gain access to a production machine without 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.
74. The organization separates duties of individuals by granting users access based on job responsibilities and least privilege, and limiting access to only authorized users.	CC5.1	Inquired of the Program Manager and determined organization separated duties of individuals by granting users access based on job responsibilities and least privilege and limiting access to only authorized users.	No deviations noted.
		Inspected relevant policies and guidelines, and determined 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 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed an attempt to grant user access to a group based on job responsibilities and least privilege by an appropriate approver and determined access was granted.	No deviations noted.
		Observed an attempt to grant user access to a group based on job responsibilities and least privilege without an appropriate approver and determined access was not granted.	No deviations noted.
		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.
75. Access to production machines, support tools, and network devices is managed via access control lists. Modifications to access control lists are recorded and approved by administrators.	CC5.2, CC6.2, CC6.3, CC6.6	Inquired of the Program Manager and determined that access to production machines, support tools, and network devices is managed via access control lists. Modifications to access control lists are recorded and approved by administrators.	No deviations noted.
		Inspected relevant documentation and determined the organization had formal procedures for managing user access to production machines, support tools, and network devices via access control lists.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the configurations within the source code management system and determined that the relevant access control list systems were configured to enforce approval from a group administrator prior to a user receiving access to production machines, support tools, and network devices.	No deviations noted.
		Observed an attempt to grant user access to a group with the appropriate approval from 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 a 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.
76. Access to corporate network, production machines, network devices, and support tools requires a unique	CC6.1, CC6.2	Inquired of the Program Manager and determined access to the corporate network, which further provides access to production machines, network devices, and support tools, required a unique ID and verified credentials.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
ID, password, and/or machine certificate.		Inspected the configuration for access to corporate network, network devices, production machines, and support tools and determined a unique ID and verified credentials were required.	No deviations noted.
		Observed a user attempt to create a user with a username belonging to another user and determined that a duplicate username could not be assigned.	No deviations noted.
		Observed a user attempt to create, delete, and recreate an account with the same username and determined the accounts were assigned unique IDs.	No deviations noted.
		Observed a user attempt to access the corporate network without verified credentials and determined access was denied.	No deviations noted.
		Observed a user attempt to access the corporate network with verified credentials and determined access was granted.	No deviations noted.
77. Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis upon	CC5.2, CC6.2, CC6.3	Inquired of the Program Manager and determined access to production machines, support tools, network devices and corporate assets was automatically removed in a timely basis upon submission of a termination request by Human Resources or a manager.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
submission of a termination request by Human Resources or a manager.		Inspected relevant documentation and determined requirements for terminating users with access to production machines, support tools, network devices and corporate assets were documented.	No deviations noted.
		Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets and determined it was configured to remove access upon submission of a termination request by Human Resources or a manager.	No deviations noted.
		Inspected the HRSync job configuration and determined that alerts were created for HRSync job failures and history shows that the job is running.	No deviations noted.
		Inspected a sample HRSync job failure and determined that failure was resolved in a timely manner.	No deviations noted.
		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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
78. Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	CC6.6	Inquired of the Program Manager and determined access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No deviations noted.
		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.
79. External system users are identified and authenticated via the Google Accounts or the BYOID authentication system before access is granted.	CC6.1	Inquired of the Program Manager and determined external system users were identified and authenticated via the Google Accounts authentication system before access is granted.	No deviations noted.
		Inspected the configuration supporting the login functionality and determined users were identified and authenticated via the Google Accounts authentication system before access was granted.	No deviations noted.
		Observed an external system user login with a valid Google account and determined access was granted.	No deviations noted.
		Observed an external system user attempt to login with an invalid Google account and determined access was denied.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
80. Where "on demand request" mechanisms are implemented to restrict human access to production resources, access requests are reviewed and approved by a second individual prior to being granted and the event is logged.	CC6.2, CC6.3	Inquired of the Program Manager and determined that "on demand request" mechanisms 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.
		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 approver group and determined changes to the approver group were recorded and approved.	No deviations noted.
		Observed an authorized user attempt to gain access to an on-demand group and determined after the request received appropriate approval from a second individual, access was granted for a limited number of hours.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed an authorized user attempt to gain access to an on-demand group and determined approval from an unauthorized user was denied.	No deviations noted.
		Observed an unauthorized user attempt to gain access to an on-demand group and determined access was denied.	No deviations noted.
81. Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	CC6.2, CC6.3	Inquired of the Program Manager and determined that critical access groups were reviewed 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 that automatically generates a ticket for the review of in scope critical access groups and determined that tickets were configured to be created 180 days after the previous review was completed.	No deviations noted.
		Inspected a sample of in-scope product and determined critical access groups were appropriately identified.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of critical access group user membership reviews performed by group administrators and determined group membership was reviewed on a semiannual basis and that appropriate action was taken to resolve inappropriate access, if applicable.	No deviations noted.
		Inspected a sample critical access group review and reperformed the review to determine that user membership was reviewed, and appropriate actions were taken to resolve inappropriate access.	No deviations noted.
82. The organization has established guidelines for protecting against the risks of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems.	CC6.1, CC6.7	Inquired of the Program Manager and determined 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	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.
83. Remote access to corporate machines requires a digital certificate issued by the organization installed on the connecting device,	CC6.1, CC6.6	Inquired of the Program Manager and determined remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
and two-factor authentication in the form of user ID, password, security key, and/or certificate.		Inspected relevant documentation and determined remote access to corporate machines required a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificates.	No deviations noted.
		Inspected the remote access configuration and determined it required a 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	Tests Performed by EY	Results
84. Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.	A1.2	Inquired of the Operations Manager and determined critical power and telecommunications equipment in data centers were physically protected from disruption and damage.	No deviations noted.
		Observed a sample of data centers and determined that power and telecommunications equipment in data centers were physically protected from disruption and damage.	No deviations noted.
		Observed a sample of data centers and determined that temperature and humidity of data halls were within the configured thresholds.	No deviations noted.
85. Storage media used for off-site redundancy are protected and controlled during transport outside of controlled areas using secure storage containers.	C1.2	Inquired of the Operations Manager and determined storage media used for off-site redundancy were protected and controlled during transport outside of controlled areas using secure storage containers.	The usage of backup tape technology related to off-site storage media began the decommissioning process in December 2021. At the time of our testing, all tapes were removed from operation. As such, there were no sample occurrences during the period.
		Observed a sample of data centers and determined that backup tapes were protected and controlled during transport outside of controlled areas using secure storage containers and that backup tapes were unmarked.	
		Inspected the relevant configuration and determined that backup tapes were encrypted.	

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the relevant configuration and determined alerts were configured to generate if thresholds for Google's sanitization or transportation processes were exceeded.	
		Inspected a sample of alerts related to unsecured tapes and determined the alerts were appropriately generated and resolved in a timely manner.	
86. Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	CC6.4	Inquired of the Operations Manager and determined information systems and equipment were safeguarded against unauthorized entry and removal from data centers and data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	No deviations noted.
		Inspected internal documentation and determined that the organization maintains policies and guidelines around the security of storage devices during delivery and movement throughout the data center.	No deviations noted.
		Observed a sample of data centers and determined that Google had safeguards in place to protect information systems and equipment from unauthorized entry and removal from data centers.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample of data centers and determined that dedicated receiving and shipping areas were isolated from the main data center floor, network rooms and security systems.	No deviations noted.
		Inspected a sample of tickets created for data center equipment entering and exiting data centers and determined Google authorized, monitored, and controlled the shipments and maintained a record of the items.	No deviations noted.
87. The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.	CC6.5, P4.3	Inquired of the Operations or Facilities Managers at each site and determined the organization sanitized storage media prior to disposal, release out of organizational control, or release for reuse.	No deviations noted.
		Inspected the data destruction and transportation policies and determined the organization had policies in place regarding the sanitization of storage media prior to disposal, release out of organizational control, or release for reuse.	No deviations noted.
		Inspected 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	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 alert 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.
88. Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.	CC6.4	Inquired of the Data Center Security Manager and determined data center perimeters were defined and secured via physical barriers. Access to sensitive data center zones required approval from authorized personnel and was controlled via badge readers, biometric identification mechanisms, or physical locks.	No deviations noted.
		Observed a sample of data centers and determined that access to sensitive data center facilities required approval from authorized personnel, and required two-factor authentication using badge readers, biometric identification mechanisms or physical locks.	No deviations noted.
		Inspected the Data Center Physical Access Policy and determined access was provisioned on a least-privileged basis and the facilities had segregated security zones.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample of data centers and determined that facilities had segregated security zones.	No deviations noted.
		Observed a sample of data centers and determined that data center perimeters were defined and secured via physical barriers.	No deviations noted.
89. Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).	CC6.2, A1.1, A1.2	Inquired of the Data Center Operations Manager and determined redundant power was utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power sources.	No deviations noted.
		Observed a sample of data centers and determined that network rooms were connected to a 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	Tests Performed by EY	Results
90. The organization records and reviews requests to store and transport removable media containing PII for security and use by authorized personnel.	CC6.7, P4.3	Inquired of the Program Manager and determined PII and SPII on removable media leaving Google facilities was approved and encrypted.	No deviations noted.
		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.
91. Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.	CC6.4	Inquired of the Data Center Security Manager and determined visitors were required to gain approval from authorized personnel, have their identity verified and remain with an escort during the duration of their visit.	No deviations noted.
		Inspected the physical security policies and determined 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of access requests to visit data centers and determined approvals were obtained from authorized personnel prior to the visits, and visitors remained with an escort during the duration of their visits.	No deviations noted.
92. Data center perimeters are defined and secured via physical barriers.	CC6.4	Inquired of the Data Center Security Manager and determined data center perimeters were defined and secured via physical barriers. Access to sensitive data center zones required approval from authorized personnel and was controlled via badge readers, biometric identification mechanisms, or physical locks.	No deviations noted.
		Observed a sample of data centers and determined that access to sensitive data center facilities required approval from authorized personnel, and required two-factor authentication using badge readers, biometric identification mechanisms or physical locks.	No deviations noted.
		Inspected the Data Center Physical Access Policy and determined access was provisioned on a least-privileged basis and the facilities had segregated security zones.	No deviations noted.
		Observed a sample of data centers and determined that facilities had segregated security zones.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample of data centers and determined that data center perimeters were defined and secured via physical barriers.	No deviations noted.
93. Automated mechanisms are utilized to track inventory of production machines and inventory of all serialized server components.	CC6.7	Inquired of the Data Center Operations Manager and determined automated mechanisms were utilized to track inventory of production machines.	No deviations noted.
		Inspected the records from the inventory system for a sample of production machines selected during data center inspections and determined the selected machines existed in the inventory system.	No deviations noted.
		Observed a sample of production machines selected from the inventory system prior to the data center inspection and determined that the selected machines existed at the data centers.	No deviations noted.
94. Data centers are equipped with fire detection alarms and protection equipment.	A1.2	Inquired of the Data Center Operations Facilities Manager and determined data centers were equipped with fire detection alarms and protection equipment.	No deviations noted.
		Observed a sample of data centers and determined that they were equipped with fire detection alarms and protection equipment.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a sample of data centers and determined that 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.
95. Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	CC5.2	Inquired of the Operations Manager and determined critical data center equipment supporting 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	Tests Performed by EY	Results
96. 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	Inquired of the Operations Manager and determined information systems and equipment were safeguarded against unauthorized entry and removal from data centers and data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	No deviations noted.
		Inspected internal documentation and determined that the organization maintains policies and guidelines around the security of storage devices during delivery and movement throughout the data center.	No deviations noted.
		Observed a sample of data centers and determined that Google had safeguards in place to protect information systems and equipment from unauthorized entry and removal from data centers.	No deviations noted.
		Observed a sample of data centers and determined that dedicated receiving and shipping areas were isolated from the main data center floor, network rooms and security systems.	No deviations noted.
		Inspected a sample of tickets created for data center equipment entering and exiting data centers and determined Google authorized, monitored, and controlled the shipments and maintained a record of the items.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
97. Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.	CC6.4	Inquired of the Program Manager and determined user access to high-security areas in data centers was reviewed on a quarterly basis and inappropriate access was removed in a timely manner.	No deviations noted.
		Inspected the internal policies and determined user access to high-security areas in data centers was reviewed on a periodic basis.	No deviations noted.
		Inspected a sample of quarterly data center access reviews and determined that reviews were performed completely and accurately in a timely manner by appropriate personnel.	No deviations noted.
		Inspected a sample of users marked as appropriate within a quarterly data center access review and determined the users were appropriate based on cost center and job title.	No deviations noted.
		Inspected a sample of inappropriate users identified as inappropriate within a quarterly data center access review and determined the users were removed in a timely manner.	No deviations noted.
98. Security measures utilized in data centers are assessed annually and the results are	CC6.4	Inquired of the Program Manager and determined security measures utilized in data centers were assessed periodically and the results were reviewed by executive management.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
reviewed by executive management.		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.
99. Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	CC6.4	Inquired of the Data Center Facilities Manager and determined that physical security measures were in place as described and are reviewed through the annual data center security review.	No deviations noted.
		Inspected a sample of data center security reviews 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	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.
100. Visitors to corporate offices must be authenticated upon arrival and remain with an escort for the duration of their visit.	CC6.4	Inquired of the Security Officer and determined that visitors to corporate offices were required to authenticate upon arrival and remain with an escort for the duration of their visit.	No deviations noted.
		Inspected internal documentation and determined the organization maintained policies for visitor access to corporate offices.	No deviations noted.
		Performed inspections for a sample of offices and determined that the reception area was isolated from the office space.	No deviations noted.
		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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
101. The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	CC6.1, CC8.1	Inquired of the Program Manager and determined the organization used an internal code management system to manage source code, documentation, release labeling, and that access to the system had to be approved.	No deviations noted.
		Inspected a sample code release configuration to determine that when created, the code released generated a name based on a set of predefined logic.	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.
		Observed a positive and a negative test and determined access to the code management system had to be approved before access was granted.	No deviations noted.
102. Changes to the organization's systems are tested before being deployed.	CC8.1	Inquired of the Program Manager to obtain an understanding of the change management process in place along with the associated tools used to make changes to in-scope products.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inquired of the Program Manager and determined that application and configuration changes in the code management system were tested, validated, and documented prior to implementation to production.	No deviations noted.
		Inspected the associated ticket details for a sample of application and configuration changes and determined that the changes were tested, validated, and documented prior to implementation to production.	No deviations noted.
		Inspected a sample of monthly reviews of changes that did not follow the automated deployment process and determined that each change included in the review was evaluated by an appropriate individual and action items were addressed timely.	No deviations noted.
103. System changes are reviewed and approved by a separate technical resource before moving into production.	CC2.1, CC8.1	Inquired of the Program Manager and determined system changes were reviewed and approved by a separate technical resource before migration to production.	No deviations noted.
		Inspected the applicable code for the internal code management system and determined system changes required a review 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	Tests Performed by EY	Results
		Inspected evidence of positive and negative testing and determined the internal code management system required changes to be reviewed by a separate technical resource before migration to production.	No deviations noted.
104. The descriptions of the organization's systems (including their scope and boundaries) are made available to internal teams.	CC2.2	Inquired of the Program Manager and determined that descriptions of the organization's systems, including their scope and boundaries, were made available to internal teams.	No deviations noted.
		Inspected the internal website for all internal products and determined 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.
105. Design documentation is required to be completed and be reviewed before a feature launch which introduces new	C1.1	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
collection, processing, or sharing of user data.		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.
106. The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	CC3.2, CC3.3, CC6.8, CC7.1, CC7.2	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	Tests Performed by EY	Results
		Inspected relevant configurations and determined vulnerabilities were tracked through an internal ticketing system and 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.
107. The organization has implemented mechanisms to protect the production environment from denial of service attacks.	CC7.2	Inquired of the Program Manager and the Security Reliability Engineer and determined there were mechanisms in place to protect the production environment against a variety of denial of service attacks.	No deviations noted.
		Inspected the documentation for mechanisms that are used to protect against denial of service attacks and determined they were in place to protect the production environment.	No deviations noted.
		Inspected playbooks used by the incident management teams and determined mechanisms were in place to classify, escalate and triage denial of service attacks.	No deviations noted.
		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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
108. Penetration tests are performed at least annually.	CC4.1	Inquired of the Program Manager and determined the organization performed penetration tests by qualified internal personnel or an external service provider at least annually.	No deviations noted.
		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	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.
109. The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	CC2.2, CC7.3	Inquired of the Program Manager and determined the organization had an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No deviations noted.
		Inspected the organization's incident response policy and determined policies and procedures were in place which outline a quick, effective, and orderly response to information security incidents. In addition, classification, prioritization, and escalation of security incidents per criticality are also identified and mechanisms are defined to measure and monitor the type and scope of security incidents.	No deviations noted.
110. The organization maintains a framework that defines how to organize a response to	CC7.3, CC7.4, P6.3	Inquired of the Program Manager and determined the organization maintained a framework that defined how to organize a response to security and privacy incidents.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
security and privacy incidents.		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.
111. Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to prevent future incidents and can be used as examples for information security training.	CC7.5	Inquired of the Program Manager and determined information security incidents were documented per the organization's Incident Response Policy. Information from these events could be used to prevent future incidents and as examples for information security training.	No deviations noted.
		Inspected the organization's Incident Response Policy and determined it documented the process for reporting, responding to, and monitoring information security incidents.	No deviations noted.
		Inspected relevant internal documentation and determined information security trainings were implemented and information from past security incidents were used as examples for the trainings to ensure these events are identified, responded to, monitored and resolved in a timely manner.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
112. 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	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.
		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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
113. The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	CC7.3, CC7.4, P6.3, P6.6	Inquired of the Program Manager and determined the organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.	No deviations noted.
		Inspected relevant documentation and determined procedures existed for users to prepare, report and investigate security and privacy incidents.	No deviations noted.
		Inspected the Cloud Data Processing Amendment and determined policies and procedures existed to notify customers of an incident in a timely manner and in accordance with applicable laws.	No deviations noted.
		Inspected a sample of data incidents and determined customers were notified of data incidents in a timely manner when required by applicable laws or contractual agreements.	No deviations noted.
		Inspected the public dashboards and tools available to customers and determined customers were notified of outages and incidents that impact relevant services.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
114. The organization has a dedicated team responsible for managing security and privacy incidents.	CC7.2, CC7.3, CC7.4, CC7.5, A1.3, P6.3	Inquired of the Program Manager and determined the organization had a dedicated team responsible for managing security and privacy incidents 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.
		Inspected a sample of incident tickets and determined the incident response team quantified and monitored incidents.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
115. The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	CC6.8, CC7.1, CC7.3, A1.1	Inquired of the program manager and determined the organization provided monitoring tools to facilitate the detection and reporting of operational issues and the monitoring tools sent automated alerts to operational personnel based on predetermined criteria and are escalated per policy.	No deviations noted.
		Inspected relevant documentation and determined there were tools in place to detect and report operational issues to operational personnel.	No deviations noted.
		Inspected a sample of alerts and determined monitoring tools were in place to detect, report, escalate and resolve operational issues.	No deviations noted.
		Inspected evidence 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.
116. The organization provides internal personnel (employees and extended workforce) with instructions and mechanisms for reporting potential security and privacy concerns or incidents to the	CC7.3, CC7.4, P6.3	Inquired of the Program Manager and determined the organization has 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
responsible team(s).		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.
		Inspected a sample of incident tickets and determined the incident response team quantified and monitored incidents.	No deviations noted.
117. The organization provides external users with mechanisms to report security issues, incidents and concerns.	CC2.3	Inquired of the Program Manager and determined that the organization provided 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the organization's websites and determined separate communication channels were in place to enable anonymous or confidential communication when the normal channels are inoperative or ineffective.	No deviations noted.
118. Security event logs are protected and access is restricted to authorized personnel.	CC6.1, CC6.2	Inquired of the Program Manager and determined security event logs were protected and access was restricted to authorized personnel.	No deviations noted.
		Inspected the system configuration related to audit logs and determined log files were not modifiable.	No deviations noted.
		Inspected internal documentation and determined policies and procedures for restriction of logical access to audit logs to authorized personnel were in place.	No deviations noted.
		Inspected a sample of members with access to audit logs and determined they were appropriate to have access to audit logs.	No deviations noted.
		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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
119. 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	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.
120. Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	CC7.2, CC7.3, CC7.4, C1.1	Inquired of the Security Engineering Manager and determined audit logs were continuously monitored for events related to security, availability, processing integrity and confidentiality threats and alerts are generated for further investigation.	No deviations noted.
		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	Tests Performed by EY	Results
		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.
121. 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	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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 of deleted products and determined an automated deletion mechanism was implemented and confidential information was disposed of as per the data retention and deletion policies.	No deviations noted.
		Inspected a sample product and determined data deletion tools verified that backup data was deleted following the configured retention period, as part of the deletion mechanism process.	No deviations noted.
122. 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	P5.1, P5.2	Inquired of the Program Manager and determined that Customers of the organization's services were provided a mechanism to access, correct, and erase PII created by their accounts.	No deviations noted.
		Inspected the Google 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
services.		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.
123. A service administrator is provided a mechanism to facilitate a service user's right to access, correct, and erase Customer Data pertaining to the user, consistent with the functionality of the services.	P5.1, P5.2	Inquired of the Program Manager and determined a Google service administrator was provided a mechanism to facilitate a Google service user's right to access, correct, and erase PII pertaining to the user.	No deviations noted.
		Inspected the Data Processing Terms and Terms of Service and determined that Google provided customers with the 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.
124. The organization's information processing resources are distributed across distinct, geographically dispersed	CC7.4, A1.1, A1.2, A1.3	Inquired of the Program Manager and determined the organization's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
processing facilities to support service redundancy, and availability.		Inspected a sample datastore configuration for a Google Workspace product and determined the product was configured to replicate to support service redundancy, and availability.	No deviations noted.
		Inspected the Google Workspace product's monitoring dashboard and determined resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy.	No deviations noted.
		Inspected a Google Workspace product's monitoring dashboard and determined resources were distributed across distinct, geographically dispersed processing facilities to support service availability.	No deviations noted.
125. Backups are periodically performed to support the availability of customer data.	A1.2	Inquired of the Program Manager and determined Google Workspace Core Services backups are periodically performed to support the availability of customer data.	No deviations noted.
		Inspected relevant documentation and determined Google Workspace Core Services backups are periodically performed to support the availability of customer data.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected the Google Workspace Core service backup configuration for each relevant Core Service and determined backups were configured to be performed periodically.	No deviations noted.
		Inspected a sample of backup logs and determined relevant Google Workspace Core Services backups were performed periodically.	No deviations noted.
126. Restore tests are periodically performed to confirm the ability to recover user data.	A1.2, A1.3	Inquired of the Program Manager and determined restore tests were periodically performed to confirm the ability to recover customer data.	No deviations noted.
		Inspected internal documentation and determined that Google Workspace services manual data restoration were outlined in the compliance requirements.	No deviations noted.
		Inspected the configuration for automated restore tests and determined tests were configured to be periodically performed to confirm the ability to recover customer data.	No deviations noted.
		Inspected a sample of automated and manual data restore tests for Google Workspace Core Services products and determined restore testing was performed periodically.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected business continuity plan documentation and determined restore tests were performed periodically as part of the business continuity plan testing.	No deviations noted.
127. Customer data that is uploaded or created is encrypted at rest.	CC6.1	Inquired of the Program Manager and determined customer data that was uploaded or created was encrypted at rest.	No deviations noted.
		Inspected the policies surrounding customer data encryption at Google and determined guidelines and policies were implemented to protect customer data.	No deviations noted.
		Inspected the encryption configuration for storage devices with customer data at rest and determined that encryption was enabled to protect customer data.	No deviations noted.
		Inspected a sample of storage devices with customer data and determined they displayed an encrypted state.	No deviations noted.
128. Integrity checks are in place at the application level to ensure data integrity.	CC6.7, CC7.1	Inquired of the Program Manager and determined integrity checks were in place via checksum verifications at the application level to help ensure data integrity.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
129. 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	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 the resource monitoring site and determined the dashboards monitor the use of resources and have the capability of projecting future capacity requirements.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of automated notifications related to critical resource capacity utilization and determined alerts were appropriately set.	No deviations noted.
130. Teams within the organization document standard operating procedures and make them available to authorized personnel.	CC2.1	Inquired of the Program Manager and determined that teams within the organization document standard operating procedures and make them available to authorized personnel.	No deviations noted.
		Inspected internal team handbooks for a sample Google Workspace product team and determined that documented standard operating procedures were in place and available to authorized personnel.	No deviations noted.
131. The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	CC9.1, A1.2, A1.3	Inquired of the Program Manager and determined that the organization conducted disaster resiliency testing (DiRT) which covered reliability, survivability, and recovery on an ongoing basis (and at least annually).	No deviations noted.
		Inspected a sample of the functional disaster resiliency testing documentation and determined that it was conducted on a periodic basis and testing was conducted to ensure continuous and automated disaster readiness, response, and recovery of business, systems and data.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
132. The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	CC9.1, A1.2, A1.3	Inquired of the Program Manager and determined that the organization had implemented business continuity measures to maintain the availability of the organization's production infrastructure and services.	No deviations noted.
		Inspected internal documentation and determined that the organization defined the risks and recovery objectives to establish measures that maintain the availability of its production infrastructure and services.	No deviations noted.
		Inspected the documentation that establishes measures to maintain the availability of the organization's production infrastructure and services.	No deviations noted.
		Inspected the documentation that establishes measures to maintain the availability of the organization's production infrastructure and services and determined the documentation was tested on an interval basis or upon significant organizational or environmental changes.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample team guideline available and determined it included the procedures which need to be followed in an emergency.	No deviations noted.
		Inspected a sample ticket and determined recovery activities were outlined.	No deviations noted.
133. The organization maintains business continuity plans to define how personnel should respond to disruptions.	CC9.1, A1.2, A1.3	Inquired of the Program Manager and determined the organization maintains business continuity plans to define how personnel should respond to disruptions.	No deviations noted.
		Inspected internal websites and determined that business continuity plans were maintained and made available to corresponding data center teams for organization-owned and third-party data centers.	No deviations noted.
		Inspected the business continuity plans related to natural disasters, weather events, and personnel threats for a sample of the Organization-owned data centers and determined the required actions and risk mitigation activities for recovering business operations due to potential business disruptions were defined.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
134. The organization's privacy program is periodically reviewed for appropriateness.	P8.1	Inquired of the Program Manager and determined the organization's privacy program was periodically reviewed for appropriateness.	No deviations noted.
		Inspected internal documentation and determined the organization's privacy program was periodically reviewed for appropriateness.	No deviations noted.
		Inspected the Internal Audit report and determined the organization's privacy program was periodically reviewed by Internal Audit for effectiveness.	No deviations noted.
135. The organization has established feedback processes that give external users the ability to voice privacy concerns, which are monitored.	P8.1	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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
136. The organization records requests to disclose user data. The organization's records of requests for user data include information regarding when the request was submitted, the identity of the requester, user data that was requested, any data that had been disclosed, and when disclosure had occurred.	P6.2	Inquired of the Program Manager and determined the organization reviewed government agency requests for customer data to determine if disclosure is required; subsequent disclosure was then limited only to that which was necessary to fulfill the request. The organization recorded and tracked transfers and disclosures of user data to third parties.	No deviations noted.
		Inspected the Google Workspace 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.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected a sample of disclosure requests in the legal request management tool and determined the organization recorded and tracked transfers and disclosure of data to third parties, and the disclosures were limited to only that which was necessary to fulfill the request.	No deviations noted.
137. Where the organization is a data processor, the organization has policies regarding its obligations to customers' ability to access, correct and/or erase their user data.	P5.1, P5.2, P6.7, P7.1	Inquired of the Program Manager and determined the organization had policies regarding its obligations to customers' ability to access, correct, and/or erase their user data.	No deviations noted.
		Inspected relevant documentation and determined the organization had policies regarding its obligations to customers' ability to access, correct, and/or erase their user data.	No deviations noted.
138. Where the organization is a data processor, the organization limits scope of processing to what is specified in contracts with the controller.	P1.1, P2.1, P3.1, P3.2, P4.1, P4.2, P7.1	Inquired of the Program Manager and determined the organization limited the scope of processing to what was specified in contracts with the controller.	No deviations noted.
		Inspected externally published documentation and determined the organization provided notice to data subjects about its privacy practices with consent obtained for the use of personal information and the organization limited the scope of processing to what was specified in contracts with controller.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Inspected internal documentation and determined the organization limited the scope of processing to what was specified in contracts with the controller.	No deviations noted.
		Observed a user upload data to Google Workspace 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.
139. Where the organization is a data processor, the organization maintains the necessary records of processing in accordance with contractual obligations to controllers.	P6.7	Inquired of the Program Manager and determined where the organization was a data processor, the organization maintained the necessary records of processing in accordance with the contractual obligations to controllers.	No deviations noted.
		Inspected the Cloud Data Processing Addendum and other internal documentation and determined where the organization was a data processor, the organization maintained the necessary records of processing in accordance with the contractual obligations to controllers.	No deviations noted.
		Inspected a sample processor record of processing for Google Workspace and determined 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	Tests Performed by EY	Results
140. The organization reviews government agency requests for user data to determine if disclosure is required; subsequent disclosure is then limited only to that which is necessary to fulfill the request.	P6.1, P6.4	Inquired of the Program Manager and determined the organization reviewed government agency requests for customer data to determine if disclosure is required; subsequent disclosure was then limited only to that which was necessary to fulfill the request. The organization recorded and tracked transfers and disclosures of user data to third parties.	No deviations noted.
		Inspected the Google Workspace 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.
141. The organization performs privacy reviews prior to product launch.	C1.1, P3.1	Inquired of the Program Manager and determined design documentation and privacy reviews, where applicable, were required to be completed prior to a product or feature launch. Any changes to customer facing services were communicated to relevant personnel and impacted customers.	No deviations noted.
		Inspected documentation and determined the organization had defined procedures and requirements for a product or feature launch.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		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.
142. The organization conducts periodic privacy risk assessments to identify and evaluate risks related to the handling of user data.	CC3.1, CC3.2, CC3.3, CC3.4, CC5.1, CC5.2, A1.3	Inquired of the Program Manager and determined the organization conducted periodic privacy risk assessments to identify and evaluate risks related to the handling of user data.	No deviations noted.
		Inspected internal documentation and determined the organization had a formal risk assessment process that included policies and procedures for identification, evaluation, ownership, treatment, and acceptance of privacy risks.	No deviations noted.
		Inspected the risk assessment and determined the organization identified and evaluated risks related to the handling of user data.	No deviations noted.
143. The organization has an incident response program for responding to privacy incidents. Privacy incidents are	P6.3, P6.5	Inquired of the Program Manager and determined the organization had an incident response program in place for responding to privacy incidents. Privacy incidents were monitored and tracked in accordance with internal policy.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
monitored 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.
144. Internal Audit performs a periodic assessment of privacy controls. Results are shared as necessary and are considered for ongoing improvement of the privacy program.	P8.1	Inquired of the Program Manager and determined Internal Audit performed a periodic assessment of privacy controls. Results were shared as necessary and were considered for ongoing improvement of the privacy program.	No deviations noted.
		Inspected internal documentation and determined Internal Audit was responsible for performing a periodic assessment of Google's privacy controls.	No deviations noted.
		Inspected the Internal Audit report and determined Internal Audit performed a periodic assessment of privacy controls. Results were shared as necessary and were considered for ongoing improvement of the privacy program.	No deviations noted.
145. Integrity checks are in place at the file system level to ensure data	CC7.1	Inquired of the Program Manager and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
integrity.		Inspected Google's security policies and determined integrity checks were in place at the file system level to ensure data integrity.	No deviations noted.
		Inspected the monitoring tool configurations and determined the tools were configured to monitor production machines and detect deviations to ensure data integrity at the file system level.	No deviations noted.
		Inspected the log of the tool used to monitor the replication of the standard production image and determined the tool was running in accordance with the schedule defined in the configuration to ensure data integrity at the file system level.	No deviations noted.
		Observed a Software Engineer insert a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
		Observed a Software Engineer modify a sample file in the directory of a haphazardly selected production machine and determined the tool detected the sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.

Criteria, Controls, Tests and Results of Tests

Control Description	SOC 2 Criteria Reference	Tests Performed by EY	Results
		Observed a Software Engineer delete a sample file in the directory of a haphazardly selected production machine and determined the tool detected the deleted sample file, confirming that integrity checks were in place at the file system level.	No deviations noted.
146. Action items identified from the results of internal audit control testing are assigned an owner and tracked to ensure remediation.	P8.1	Inquired of the Program Manager and determined action items identified from the results of internal audit control testing were assigned an owner and tracked to ensure remediation.	No deviations noted.
		Inspected the internal audit report and determined action items identified from the results of internal audit control testing were assigned an owner and tracked to ensure remediation.	No deviations noted.
		Inspected action items from prior year internal audit testing and determined they were assigned an owner and tracked to ensure remediation.	No deviations noted.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC1.1 - COSO Principle 1		
CC1.1	5, 6, 9, 11, 52	The entity demonstrates a commitment to integrity and ethical values.
CC1.2 - COSO Principle 2		
CC1.2	3	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	1, 2, 7, 10	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	1, 10, 11, 52	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5 - COSO Principle 5		
CC1.5	2, 3, 4, 6	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.1 - COSO Principle 13		
CC2.1	40, 48, 103, 130	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2 - COSO Principle 14		
CC2.2	2, 32, 33, 39, 40, 48, 52, 104, 109	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	30, 31, 32, 33, 34, 117	The entity communicates with external parties regarding matters affecting the functioning of internal control.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC3.1 - COSO Principle 6		
CC3.1	2, 14, 15, 16, 142	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	14, 15, 16, 41, 106, 112, 142	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	14, 15, 16, 106, 142	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4 - COSO Principle 9		
CC3.4	14, 15, 16, 142	The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.1 - COSO Principle 16		
CC4.1	17, 19, 51, 108	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	17, 19	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	14, 15, 18, 74, 142	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	8, 14, 15, 18, 35, 75, 77, 95, 142	The entity also selects and develops general control activities over technology to support the achievement of objectives.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC5.3 - COSO Principle 12		
CC5.3	19, 35, 38, 39, 47, 51	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.1		
CC6.1	41, 42, 46, 53, 54, 56, 58, 60, 61, 63, 69, 71, 72, 73, 76, 79, 82, 83, 101, 118, 121, 127	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	56, 70, 75, 76, 77, 80, 81, 89, 118	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	70, 75, 77, 80, 81	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	43, 86, 88, 91, 92, 97, 98, 99, 100	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		
CC6.5	87	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.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC6.6		
CC6.6	59, 63, 68, 73, 75, 78, 83	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7		
CC6.7	43, 44, 45, 49, 50, 63, 64, 68, 82, 90, 93, 96, 128	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	62, 65, 106, 115, 119	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	55, 57, 106, 115, 128, 129, 145	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	14, 106, 107, 114, 119, 120, 129	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	109, 110, 113, 114, 115, 116, 119, 120, 129	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.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
CC7.4		
CC7.4	110, 113, 114, 116, 119, 120, 124, 129	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	47, 111, 114, 119, 129	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.1		
CC8.1	36, 49, 66, 67, 101, 102, 103, 119	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, 131, 132, 133	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2		
CC9.2	5, 12, 13, 21, 22, 23, 24, 25, 37	The entity assesses and manages risks associated with vendors and business partners.
A1.1		
A1.1	89, 115, 119, 124	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	84, 89, 94, 124, 125, 126, 131, 132, 133	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.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
A1.3		
A1.3	14, 114, 124, 126, 131, 132, 133, 142	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
C1.1		
C1.1	5, 7, 12, 13, 21, 22, 25, 30, 42, 46, 105, 120, 121, 141	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2		
C1.2	42, 85, 121	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
P1.1		
P1.1	26, 27, 138	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	26, 138	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	27, 138, 141	Personal information is collected consistent with the entity's objectives related to privacy.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
P3.2		
P3.2	138	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	27, 46, 138	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.
P4.2		
P4.2	26, 42, 121, 138	The entity retains personal information consistent with the entity's objectives related to privacy.
P4.3		
P4.3	26, 42, 50, 87, 90, 121	The entity securely disposes of personal information to meet the entity's objectives related to privacy.
P5.1		
P5.1	122, 123, 137	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	122, 123, 137	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.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
P6.1		
P6.1	21, 23, 28, 29, 140	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.
P6.2		
P6.2	136	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.
P6.3		
P6.3	110, 113, 114, 116, 143	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	21, 23, 29, 140	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	21, 143	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	21, 113	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

Criteria to Controls Mapping

Criteria	Controls List	Criteria
P6.7		
P6.7	28, 137, 139	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	137, 138	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	134, 135, 144, 146	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.

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.