System and Organization Controls (SOC) 3

Report on the G Suite, Other Google Services and Supporting Services System

Relevant to Security, Availability, and Confidentiality

For the Period 1 May 2018 to 30 April 2019

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Management's Report of its Assertion on the Effectiveness of Its Controls Over the G Suite, Other Google Services and Supporting Services System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

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

- Identifying the G Suite, Other Google Services and Supporting Services System (System) and describing the boundaries of the System, which are presented in Attachment A, B
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment C
- Identifying, designing, implementing, operating, and monitoring effective controls over the G Suite, Other Google Services and Supporting Services System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period 1 May 2018 to 30 April 2019 to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

Google LLC
10 September 2019

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

Report of Independent Accountants

To the Management of Google LLC:

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of Its Controls over the G Suite, Other Google Services and Supporting Services System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality" (Assertion), that Google's controls over the G Suite, Other Google Services and Supporting Services System (System) were effective throughout the period 1 May 2018 through 30 April 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Management Responsibilities

Google's management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the G Suite, Other Google Services and Supporting Services (System) and describing the boundaries of the System
- Identifying its principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of its system
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Google's

Building a better working world

relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

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

Inherent limitations

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

Opinion

In our opinion, Google's controls over the system were effective throughout the period 1 May 2018 through 30 April 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst + Young LLP

10 September 2019
San Jose, CA

Attachment A - G Suite, Other Google Services and Supporting Services System

Google Overview

Google LLC (“Google” or “the Company”) 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 web site one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world’s largest online indexes of web sites 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 G Suite and Other Google 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.

G Suite and Other Google Services 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 comprised of communication, productivity, collaboration and security tools that can be accessed from virtually 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.

G Suite Editions & SKUs

See **Attachment B** for a mapping of G Suite Products to their respective Editions or SKUs.

"G Suite Basic" is an edition of G Suite comprised of the G Suite Services, excluding Google Vault and Google Voice, which are available at additional cost, and Google Cloud Search.

"G Suite Business" is an edition of G Suite comprised of all the G Suite Services, except Google Voice, and data region policy settings for primary data within Customer Data for certain Services. Customers that have 5 or more end users will receive unlimited Google Drive storage. Customers that have 4 or fewer end users will receive 1TB of Google Drive storage for each End User.

"G Suite (Team Managed)" is an edition of G Suite offered under the G Suite Team Managed Agreement (prior version: Google Apps for Work Team Managed Agreement) which is comprised of Google Drive, Google Hangouts, Google Contacts, and Google+. Other G Suite Core Services are not available for team-managed accounts. Customers that have 5 or more end users will

receive unlimited Google Drive storage. Customers that have 4 or fewer end users will receive 1TB of Google Drive storage for each End User.

"G Suite for Education" is a free edition of G Suite comprised of the G Suite Services, excluding Google+, Google Voice, and Google Cloud Search. Customers that have 5 or more end users will receive unlimited Google Drive storage. Customers that have 4 or fewer end users will receive 1TB of Google Drive storage for each End User. This edition also includes Classroom and Chrome Sync as G Suite Core Services.

"Drive Enterprise" is an edition of G Suite comprised of Google Drive (including data loss prevention functionality) and the following as used in conjunction with Google Drive: (a) Cloud Identity Management; (b) Google Contacts; (c) Google Docs, Google Sheets, Google Slides and Google Forms; (d) Google Groups for Business; (e) Google Keep; (f) Google Sites; (g) Google Vault; (h) data region policy settings for primary data within Customer Data for certain Services; and (i) certain enhanced security and control features, migration tools, and mobile device management functionality for Administrators.

The G Suite, Other Google Services and Supporting Services covered in this system description consist of the following:

G Suite Core Services

G Suite Core Services is a set of applications, including Gmail, Docs, Sheets, Slides, Sites, and more, as well as a set of messaging, collaboration, security, and compliance tools for organizations.

Admin Console

The Google Admin Console is a management tool provided by Google for G Suite administrators. It allows administrators to maintain all their G Suite services from one dashboard. With the Google Admin Console, administrators can configure settings for G Suite, monitor the usage of their domains, create user accounts, and more.

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 for other end users, and schedule rooms and resources.

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 G Suite 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 Core Services for G Suite and select third parties. Google Cloud Search also provides end users with actionable information and recommendations.

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.

Docs

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

Drive

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

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 Forms

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

Google+

Google+ is a web-based service that allows end users to share links, videos, pictures, collections, and other content with others within the same G Suite domain, and to view and interact with content shared with them by others within that same domain.

Groups

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.

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.

Hangouts Chat

Hangouts 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.

Hangouts Meet

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

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.

Keep

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

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.

Sheets

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

Sites (Classic/New)

Sites allows a customer End User to create websites on the G Suite Basic domain to publish internally within a company or publish externally. An End User can 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.

Slides

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

Talk

Google Talk is an instant messaging service that provides both text and voice communication. Google Talk is a legacy offering available to a select set of customers.

Tasks

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

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.

Voice

Google Voice is an admin-managed 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.

G Suite Developer Offerings

A collection of tools and resources that let you integrate your software with G Suite and its users or create new apps that run entirely within G Suite. The developer offerings included in this system description includes Product APIs and Admin Software Development Kits (SDK)

Product APIs

Calendar API

Calendar API enables for 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

The Google Drive Activity API lets a customer’s app retrieve information about a user's Google Drive activity. This API provides additional functionality on top of the existing Drive API.

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.

Email Settings API

The Email Settings API enables administrators to programmatically manipulate most user-level Google Mail settings.

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.

Sheets API

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

Sites API

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

Tasks API

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

Admin SDK

Apps Email Audit API

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

Directory API

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

Domain Shared Contacts API

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

Enterprise License Manager API

The License Manager API allows administrators to manage license assignments for G Suite services in use by the organization.

Groups Migration API

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

Groups Settings API

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

Reports API

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

Reseller API

The Reseller API lets reseller administrators place customer orders and manage monthly post-pay 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.

Additional Google Services for G Suite

App Maker

App Maker is a web-based service that provides an application development environment for end users to build and deploy custom web applications.

Google Apps Script

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

Infrastructure

G Suite, Other Google Services and Supporting Services runs in a multi-tenant, distributed environment. 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 G Suite, Other Google Services and Supporting Services, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Customer data is then stored in large distributed databases, built on top of this file system.

Data Centers and Redundancy

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

Redundant architecture exists such that data is replicated in real-time to at least two (2) geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Google uses 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.

Authentication and Access

Strong authentication and access controls are implemented to restrict access to G Suite, Other Google Services and Supporting Services production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates, which helps to

positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Data traffic is encrypted between Google production facilities.

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 which utilizes Secure Shell (SSH) and TLS certificates help provide secure and flexible access mechanisms. These mechanisms are designed to grant access rights to systems and data only to authorized users.

Both user and internal access to customer data is restricted through the use of unique user account IDs. Access to sensitive systems and applications requires two-factor authentication in the form of unique user account IDs, strong passwords, security keys and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semi-annual basis under the direction of the group administrators.

As part of Google's operations, Google identified two cases where unhashed G Suite user account passwords were stored in their secure encrypted infrastructure. Google remediated these issues and followed established internal processes to notify the affected user base. Other security controls such as encryption, access control and audit logging were in place to mitigate risk of misuse and Google found no evidence of misuse of these passwords. For additional details, please refer to Google's blog post **here**.

Change Management

Change Management policies, including security code reviews and emergency fixes, are in place, and procedures for tracking, testing approving, and validating changes are documented. Changes are developed utilizing the code versioning tool to manage source code, documentation, release labeling and other functions. Google requires all code changes to be reviewed and approved by a separate technical resource, other than the developer, to evaluate the quality and accuracy of changes. Further, all application and configuration changes are tested prior to migration to production environment. Following successful pass of tests, multiple binaries are then grouped into a release and deployed to production.

Data

Google provides controls at each level of data storage, access, and transfer. Google has established training programs for privacy and information security to support data confidentiality. All employees are required to complete these training programs annually. All product feature launches that include new collection, processing, or sharing of user data are required to go through an internal design review process. Google has also established incident response processes to report and handle events related to confidentiality. Google establishes agreements, including non-disclosure agreements, for preserving confidentiality of information and software exchange with external parties.

Network Architecture and Management

The G Suite, Other Google Services and Supporting Services system architecture utilizes a fully redundant network infrastructure. Google has implemented perimeter devices to protect the Google network from external attacks. Network monitoring mechanisms are in place to detect and disconnect access to the Google network from unauthorized devices.

People

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

Formal organizational structures exist and are available to Google employees on the Company's intranet. The intranet provides drill-down functionality for identifying employees in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Policies and procedures are reviewed and updated as necessary.

Attachment B - Mapping of G Suite Products to Editions or SKUs

Product	Core Services	Basic	Business	Business (Team Managed)	Enterprise	Education	Cloud Identity	Drive Enterprise
Admin Console	✓	✓	✓		✓	✓	✓	✓
Calendar	✓	✓	✓		✓	✓		
Classroom						✓		
Cloud Identity Services	✓						✓	
Cloud Search	✓		✓		✓			
Contacts	✓	✓	✓	✓	✓	✓	✓	✓
Docs	✓	✓	✓	✓	✓	✓		✓
Drive	✓	✓	✓	✓	✓	✓		✓
Forms	✓	✓	✓	✓	✓	✓		✓
Gmail	✓	✓	✓		✓	✓		
Google Apps Script		✓	✓	✓	✓	✓		✓
App Maker		✓	✓	✓	✓	✓		✓
Google+	✓	✓	✓	✓	✓			
Groups	✓	✓	✓		✓	✓	✓	✓
G Suite Admin SDK		✓	✓	✓	✓	✓	✓	✓
G Suite Product APIs		✓	✓	✓	✓	✓		
Hangouts	✓	✓	✓	✓	✓	✓		
Hangouts Chat	✓	✓	✓	✓	✓	✓		
Hangouts Meet	✓	✓	✓	✓	✓	✓		
Jamboard	✓	✓	✓		✓	✓		
Keep	✓	✓	✓		✓	✓		
Mobile Device Management	✓	✓	✓		✓		✓	✓
Sheets	✓	✓	✓	✓	✓	✓		✓
Slides	✓	✓	✓	✓	✓	✓		✓
Talk	✓	✓	✓		✓	✓		
Tasks	✓	✓	✓		✓	✓		
Vault	✓		✓		✓	✓		✓
Voice*	✓				✓			

Attachment C - Principal Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of G Suite, Other Google Services and Supporting Services. Commitments to customers are communicated via Terms of Service, G Suite, Other Google Services and Supporting Services Service Level Agreements, and Data Processing Addendums.

System Requirements

Google has established internal policies and processes to support the delivery of the G Suite, Other Google Services and Supporting Services 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 functioning of system requirements defined by Google.

The following processes and system requirements function to meet Google's commitments to customers with respect to the terms governing the processing and security 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 all Google Applications, Systems, and Services.
- Incident Management: Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.
- Data Management: Google complies with any obligations applicable to it with respect to the processing of personal data. Google processes data in accordance with the customer instructions and complies with applicable regulations.
- Data Security: Google implements and maintains 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 sub-processors to the extent applicable to their scope of performance.
- Third Party Risk Management: Google conducts routine inspections of sub-processors to evaluate control conformance. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from sub-processors to comply with these practices.