System and Organization Controls (SOC) 3

Report over the Tables System

Relevant to Security and Availability

For the Period 1 November 2020 to 30 April 2021

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Tables System Based on the Trust Services Criteria for Security and Availability

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

- Identifying the Tables System (System) and describing the boundaries of the System, which are presented in **Attachment A**
- Identifying our service commitments and system requirements
- Identifying the risks that would threaten the achievement of its service commitments and system requirements that are the objectives of our System, which are presented in **Attachment B**
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements
- 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 November 2020 to 30 April 2021, to provide reasonable assurance that the service commitments and system requirements were achieved based on the criteria relevant to security and availability set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* only if complementary user entity controls (presented in **Attachment C**) assumed in the design of Google's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Assertion does not extend to controls of user entities.

Very truly yours,

Google LLC
12 July 2021

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

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

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 Tables System Based on the Trust Services Criteria for Security and Availability" (Assertion), that Google's controls over the Tables System (System) were effective throughout the period 1 November 2020 to 30 April 2021, to provide reasonable assurance that its service commitments and system requirements were achieved based on the criteria relevant to security and availability (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.*

The description of the boundaries of the System, which is presented in the accompanying "Attachment A – Tables System" (Description) indicates Google's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls (presented in **Attachment C**) 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.

Management's Responsibilities

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

- Identifying the System and describing the boundaries of the System
- Identifying its service commitments and system requirements and the risks that would threaten the achievement of its 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 service commitments and system requirements

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 (AICPA). 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 relevant security and availability 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 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 management assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria, if user entities applied the complementary controls assumed in the design of Google's controls throughout the period 1 November 2020 to 30 April 2021.

Ernst & Young LLP

12 July 2021
San Jose, CA

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Attachment A - Tables System

Google Overview

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.

Tables is a lightweight collaborative database with simple automation features. It helps to track and automate tasks, enabling users to save time and work smarter with features such as connecting data to reduce data entry, configuring separate views, automating updates and emails.

It can be used for a wide range of activities from project and task management, IT operations, customer tracker & sales CRM to product launch and development.

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 the Tables System:

- 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
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Delhi, India
- 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

- Ghlin, Hainaut, Belgium
- Hamina, Finland
- Henderson (NV), United States of America
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Jakarta, Indonesia
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- London (1), United Kingdom
- London (2), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom
- London (5), United Kingdom
- London (6), United Kingdom
- Los Angeles (CA), United States of America
- Melbourne, Victoria, Australia
- Middenmeer, Netherlands
- Midlothian (TX), United States of America
- Moncks Corner (SC), United States of America
- Montreal, Quebec, Canada
- Mumbai, India
- New Albany (OH), United States of America
- Osaka, Japan
- Osasco, Brazil
- Papillion (NE), United States of America
- Pryor Creek (OK), United States of America
- Quilicura, Santiago, Chile
- Salt Lake City (UT), United States of America
- Seoul, South Korea
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Toronto, Ontario, Canada
- Vinhedo, Brazil
- Warsaw (1), Poland
- Warsaw (2), Poland
- Wenya, Singapore
- Widows Creek (AL), United States of America
- Zurich, Switzerland

Infrastructure

Tables 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. This is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. User entity 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 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 Tables 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 a unique user account ID, 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 semiannual basis under the direction of the group administrators.

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 quality and accuracy of changes. Further, all application and configuration changes are tested prior to migration to the production environment. Following a 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. 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.

Network Architecture and Management

The Tables 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 prevent access to the Google network from unauthorized devices.

People

Google has implemented a process-based service quality environment designed to deliver their products. 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 and availability 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 - Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Tables System. Commitments to users are communicated via Terms of Service, Tables Service Level Agreements, and Data Processing Addendums.

System Requirements

Google has implemented a process-based service quality environment designed to deliver the Tables System. 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 users with respect to the services provided:

- 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 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

Attachment C – Complementary User Entity Controls

Tables' Services are 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.

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

Organization and Administration Controls

- Customers are responsible for ensuring their information security requirements are considered in the use of Tables including any APIs and integrations
- Customers are responsible for establishing organizational policies and procedures for the installation of third-party services
- Customers are responsible for reviewing their information security policies and the security capabilities of Tables including any APIs and integrations to determine their applicability to modify or add policies as appropriate
- Customers are responsible for establishing, documenting, and reviewing policies and procedures addressing transfer and sharing of information within their organization and with external parties
- Customers are responsible for ensuring that end-users are trained on the organizational policies and procedures relevant to Tables including any APIs and integrations
- Customers are responsible for defining, documenting, and making available to users operating procedures for the operation of Tables including any APIs and integrations

Logical Access Controls

- Customers are responsible for establishing, documenting, and reviewing policies and procedures addressing the Customer's administration of access to Tables including any APIs and integrations
- Customers are responsible for provisioning service availability, user roles, and sharing
- permissions within Tables including any APIs and integrations consistent with organizational policies
- Customers are responsible for provisioning, maintaining, and disabling users' access in accordance with their internal access management policies
- Customers are responsible for implementing secure log-on procedures to access Tables including any APIs and integrations consistent with their access policies
- Customers are responsible for reviewing users' access rights periodically, consistent with organizational policies
- Customers are responsible for enforcing the use of two-step verification on all accounts
- Customers are responsible for removing users' access rights consistent with organizational policies

- Customers are responsible for establishing procedures to allocate the initial password to access Tables including any APIs and integrations to end-users when Google password authentication is used
- Customers are responsible for training users on the use and disclosure of passwords used to authenticate to Tables including any APIs and integrations
- Customers are responsible for assigning responsibilities for the operation and monitoring of Tables including any APIs and integrations
- Customers are responsible for configuring domain settings related to integration with Tables including any APIs and integrations consistent with customer policies

Change Management Controls

- Customers are responsible for ensuring that individuals creating and/or updating profiles or accessing Tables including any APIs and integrations have the proper authorization
- Customers are responsible for reviewing and testing, as appropriate, feature and product releases and evaluating their impact consistent with their organization's needs
- Customers are responsible for periodically reviewing the configuration of Tables including any APIs and integrations to ensure it is consistent with their policies and procedures

Physical Security Controls

- Customers are responsible for ensuring the appropriate physical security controls of all devices that access Tables including any APIs and integrations

Incident Management Controls

- Customers are responsible for establishing responsibilities and procedures to respond to relevant information security incidents pertaining to the use of Tables including any APIs and integrations
- 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 Tables including any APIs and integrations
- Customers should contact Tables if there are any issues with service availability or security, including, but not limited to, unauthorized use of their password or account compromised, data and security events etc.

Availability Controls

- Customers are responsible for maintaining business continuity plans, including disaster recovery and backup procedures pertaining to the use of Tables including any APIs and integrations