System and Organization Controls (SOC) 3

Report on the Google Cloud Platform System

Relevant to Security, Availability, and Confidentiality

For the Period 1 May 2018 to 31 October 2018

SECTION I - Management's Assertion Regarding the Effectiveness of Its Controls Over the Google Cloud Platform System Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Management's Assertion Regarding the Effectiveness of Its Controls Over the Google Cloud Platform System Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

We, as management of, Google LLC ("Google" or "the Company") are responsible for designing, implementing and maintaining effective controls over the Google Cloud Platform System (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period 1 May 2018 to 31 October 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability, and confidentiality (Control Criteria) set forth in the American Institute of Certified Public Accountants' TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period 1 May 2018 to 31 October 2018 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Google's commitments and system requirements

- the System was available for operation and use, to achieve Google’s commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Google’s commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Google Cloud Platform System identifies the aspects of the Google Cloud Platform covered by our assertion.

Very truly yours,

GOOGLE LLC
14 December 2018

SECTION II - Report of Independent Accountants

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

Management of Google LLC:

Approach

We have examined management's assertion that Google maintained effective controls to provide reasonable assurance that:

- the Google Cloud Platform System was protected against unauthorized access, use, or modification to achieve Google's commitments and system requirements
- the Google Cloud Platform System was available for operation and use to achieve Google's commitments and system requirements
- the Google Cloud Platform System information is collected, used, disclosed, and retained to achieve Google's commitments and system requirements

during the period 1 May 2018 through 31 October 2018 based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Google's management. Our responsibility is to express an opinion 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 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 and appropriate 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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, and confidentiality are achieved.

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. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, Google's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality.

Ernst + Young LLP

14 December 2018
San Jose, CA

SECTION III - Description of the Google Cloud Platform System

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

Cloud Healthcare Search, as a product offered in Google Cloud Platform, is the sole scope of this report for the period 1 May 2018 through 31 October 2018.

Cloud Healthcare Search

Cloud Healthcare Search is a clinician-focused search engine over a patient's longitudinal record. The product offers comprehensive search across all resources in the record along with query expansion, suggest, and spell correction. The externally-accessible provider-facing user interface is vendor-neutral and can be used directly or embedded within an electronic health record system.

Note: Cloud Healthcare Search is the only product included in this Google Cloud Platform system description; other products may be covered as part of separate reports.

Infrastructure

Google Cloud Platform 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 Google Cloud Platform, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. Customer data is then stored in large distributed databases, built on top of this file system.

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 Google Cloud Platform production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) 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 semi-annual 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 production environment.

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 Google Cloud Platform 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 and disconnect access to the Google network from unauthorized devices.

People

Google has implemented a process-based service quality environment designed to deliver the Google Cloud Platform 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.