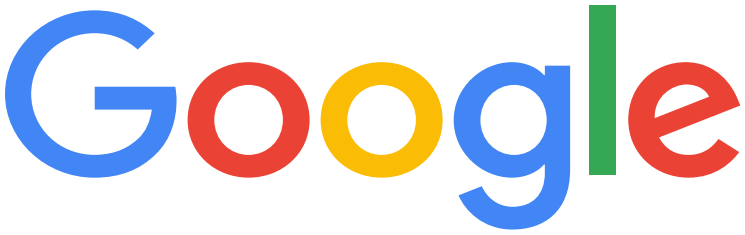

System and Organization Controls (SOC) 3 Report

Report on the Google Firebase System

Relevant to Security, Availability, Processing Integrity, and Confidentiality

For the Period 31 January 2017 to 31 October 2017

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 Firebase System Based on the Trust Services Principles and Criteria for Security, Availability, Processing Integrity, and Confidentiality

We, as management of, Google LLC ("Google" or "the Company") are responsible for designing, implementing and maintaining effective controls over the Google Firebase 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 31 January 2017 to 31 October 2017, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability, processing integrity, and confidentiality (Control Criteria) set forth in the AICPA's 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 31 January 2017 to 31 October 2017 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 processing is complete, valid, accurate, timely, and authorized 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 Firebase System identifies the aspects of the Google Firebase System covered by our assertion.

Very truly yours,

Google LLC

9 January 2018

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:

Approach:

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

- the Google Firebase System was protected against unauthorized access, use, or modification to achieve Google's commitments and system requirements
- the Google Firebase System was available for operation and use to achieve Google's commitments and system requirements
- the Google Firebase System processing is complete, valid, accurate, timely, and authorized to achieve Google's commitments and system requirements
- the Google Firebase System information is collected, used, disclosed, and retained to achieve Google's commitments and system requirements

during the period 31 January 2017 to 31 October 2017 based on the criteria for security, availability, processing integrity, 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, processing integrity 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.

Building a better working world

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, processing integrity 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 assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, processing integrity and confidentiality.

Ernst & Young LLP

9 January 2018

Description of the Google Firebase System

Google Overview

Google LLC ("Google") 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 offers Internet-based services and tools that user entities can access to communicate, collaborate, and work more efficiently. The following Google product offerings automatically save all work performed by user entities in the cloud and enable user entities to work securely, regardless of where they are in the world and what device they are using.

Google Firebase is a mobile app platform (platform-as-a-service) with an integrated, unified Software Development Kit ("SDK"). Firebase offers high-level services to help developers rapidly build applications: authentication, static hosting, notifications delivery, Android device cloud testing lab, crash reporting, real-time database (the original Firebase offering), cloud functions, durable links, app indexing, analytics, remote configurations (key-value store), app invites, and Google AdMob. The following products are included within the scope of this report for the Google Firebase System:

- Firebase Analytics
- Firebase App Invites
- Firebase Console
- Firebase Authentication
- Firebase Crash Reporting
- Firebase Real-time Database
- Firebase Dynamic Links
- Firebase Functions
- Firebase Hosting
- Firebase Cloud Messaging
- Firebase Notifications
- Firebase Performance Monitoring*
- Firebase Remote Config
- Cloud Firestore for Firebase*
- Cloud Storage for Firebase
- Firebase Test Lab for Android

*Indicates products in scope for the period 1 May 2017 through 31 October 2017

Firebase provides developers with a rich suite of tools and resources to develop and manage high quality apps, for growing their user base, and to monetize the platform. It consists of complementary features that work independently, or can be mix-and-matched as needed.

Leveraging the Google Cloud, Firebase 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.

The Google Firebase platform covered in this system description consist of the following services:

Firebase Analytics

Firebase Analytics is a fully managed data analysis service that enables businesses to analyze Big Data. It features highly scalable data storage that accommodates up to hundreds of terabytes. It enables companies to import multi-terabyte datasets, query interactively and securely share the results within their organization.

Firebase App Invites

Firebase App Invites makes it simple for users to send content to their friends, over both SMS and email, by ensuring that referral codes, recipe entries, or other shared content gets passed along with the invitation.

Firebase Console

Firebase Console is the unified web developer console for all Firebase services and helps developers get started, configure and use Firebase services.

Firebase Authentication

Firebase Authentication is a fully managed user identity system which provides backend services, easy-to-use SDKs and ready-made UI libraries to authenticate users to their application.

Firebase Crash Reporting

Firebase Crash Reporting creates detailed reports of the errors users see in their apps. In addition to automatic reports, developers can log custom events.

Firebase Real-time Database

Firebase Real-time Database is a hosted NoSQL cloud database. Data is synced across all clients in real time, and remains available when the app goes offline.

Firebase Dynamic Links

Firebase Dynamic Links are smart URLs that allow user entities to send existing and potential users to any location within their iOS or Android app. Firebase Dynamic Links survive the app install process, so even new users will see the content they’re looking for when they open the app for the first time.

Firebase Functions

Firebase Functions lets user entities run their own backend code that executes automatically based on Firebase and Google Cloud events. With Firebase Functions there's no need for user entities to manage their own server. User entity functions are stored in Google's cloud and run in a managed Node.js environment.

Firebase Hosting

Firebase Hosting is developer-focused static web hosting for modern front-end web applications. Using Firebase Hosting, developers can deploy SSL-enabled web apps to a global content-delivery network from a single command.

Firebase Cloud Messaging

Firebase Cloud Messaging ("FCM") is a cross-platform messaging solution that lets app developers reliably send messages to their users.

Firebase Notifications

Firebase Notifications is a service that allows mobile app developers to send targeted user notifications.

Firebase Performance Monitoring

Firebase Performance Monitoring is a service that helps user entities gain insight into the performance characteristics of their iOS and Android apps.

Firebase Remote Config

Firebase Remote Config enables developers to configure apps from the Firebase Console and to target configuration variations based on app and device properties. Firebase Remote Config enables staged introduction of features and customization.

Cloud Firestore for Firebase

Cloud Firestore is a flexible, scalable database for mobile, web, and server development from Firebase and Google Cloud Platform. Like Firebase Real-time Database, it keeps data in sync across client apps through real time listeners and offers offline support for mobile and web so user entities can build responsive apps.

Cloud Storage for Firebase

Cloud Storage for Firebase is a storage service built for app developers who need to store and serve user-generated content, such as photos or videos.

Firebase Test Lab for Android

Firebase Test Lab for Android provides cloud-based infrastructure for testing apps on physical and virtual devices. With a single operation, developers can test their apps across a wide variety of devices.

Infrastructure

Google Firebase 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 Firebase, 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 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 users 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.

Firebase Hosting and Firebase Real-time Database backups are periodically performed to support the availability of user entity data. Firebase Hosting and Firebase Real-time Database data restore tests are periodically performed to confirm the ability to recover customer data. Critical data is replicated to at least two (2) data centers and provides high availability by dynamically load balancing across those sites.

Authentication and access

Strong authentication and access controls are implemented to restrict access to Google Firebase production systems, internal support tools, and customer data. Machine-level access restriction relies on a certificate-based distributed authentication service, 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 ID, strong passwords, One-Time-Passwords ("OTP"), 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 groups are annually reviewed.

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 Firebase 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 unauthorized access to the Google network from unauthorized devices.

People

Google has implemented a process-based service quality environment designed to deliver the Google Firebase 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's repeatable process model includes key infrastructure and product related processes and controls over security, availability, process integrity, and confidentiality.

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.