



---

**System and Organization Controls (SOC) 3  
Report on the Google Cloud Platform System  
Relevant to Security, Availability, and Confidentiality  
For the Period 1 November 2017 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 November 2017 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 November 2017 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**  
21 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 November 2017 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*

21 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.

It includes the following services, hereafter described collectively as "Google Cloud Platform" or (GCP):

#### Big Data

- BigQuery
- BigQuery Data Transfer Service
- Cloud Dataflow
- Cloud Datalab
- Cloud Dataproc
- Cloud Pub/Sub
- Genomics

#### Compute

- App Engine
- Cloud Functions
- Compute Engine
- Kubernetes Engine

#### Cloud AI

- Cloud AutoML Natural Language\*
- Cloud AutoML Translation\*
- Cloud AutoML Vision\*
- Cloud Talent Solution
- Cloud Machine Learning Engine
- Cloud Natural Language API

- Cloud Speech-to-Text
- Cloud Text-to-Speech\*
- Cloud Translation API
- Cloud Vision API
- Dialogflow Enterprise Edition
- Cloud Video Intelligence API

#### Developer Tools

- Cloud SDK
- Cloud Source Repositories
- Cloud Build
- Container Registry

#### Management Tools

- Cloud Billing API
- Cloud Console
- Cloud Deployment Manager
- Cloud Console Mobile App
- Cloud Shell
- GCP Marketplace
- Stackdriver Debugger
- Stackdriver Error Reporting
- Stackdriver Logging
- Stackdriver Profiler
- Stackdriver Trace

#### Networking

- Cloud Armor
- Cloud CDN
- Cloud DNS
- Cloud Router
- Cloud VPN
- Cloud Interconnect
- Cloud Load Balancing
- Virtual Private Cloud (VPC)

#### Identity and Security

- Data Loss Prevention API
- Cloud Identity and Access Management
- Cloud Key Management Service

- Cloud HSM\*
- Cloud Resource Manager
- Cloud Security Scanner

#### Storage and Databases

- Cloud Bigtable
- Cloud Datastore
- Cloud Firestore
- Cloud Memorystore\*
- Cloud Spanner
- Cloud SQL
- Cloud Storage
- Cloud Storage Transfer Service
- Persistent Disk

#### Other

- Cloud Endpoints
- Cloud Healthcare API
- Cloud Identity-Aware Proxy
- Cloud IoT Core
- Google Service Control
- Orbitera
- Service Consumer Management API
- Service Management API

\*Indicates products in scope for the period 1 May 2018 through 31 October 2018

Google's product offerings for Google Cloud Platform 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 Cloud Platform is targeted towards small and medium size business, and large corporates alike, as well as the development teams within those organizations. These products provide a comprehensive variety of technical services that organizations rely on:

- Big Data - tools to capture, process, store and analyze data on a single platform
- Compute - a scalable range of computing options tailored to match the size and needs of an organization
- Cloud AI - fast, scalable and easy to use modern machine learning services, with pre-trained models and the ability to generate tailored models

- Developer Tools - a rich collection of tools and libraries that help development teams work quickly and effectively
- Management Tools - manage apps on GCP with a web-based console, mobile app, or Cloud Shell for real time monitoring, logging, diagnostics, and configuration
- Networking - a high quality private network using software-defined networking and distributed systems technologies to host and deliver services around the world
- Identity and Security - manage the security and access to cloud assets, supported by Google's own protection of its infrastructure
- Storage and Databases - scalable storage options and varieties for different needs and price points

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.

The Google Cloud Platform products covered in this system description consist of the following services:

### *BigQuery*

BigQuery 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, the ability to perform ad hoc queries on multi-terabyte datasets, and the ability to share data insights via the web.

### *BigQuery Data Transfer Service*

BigQuery Data Transfer Service automates data movement from SaaS applications to BigQuery on a scheduled, managed basis. With the BigQuery Data Transfer Service, customers can transfer data to BigQuery from SaaS applications including Google Ads, Campaign Manager, Ad Manager, and YouTube.

### *Cloud Dataflow*

Cloud Dataflow is a fully managed service for strongly consistent, parallel data-processing pipelines. It provides a Software Development Kit (SDK) for Java with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the lifecycle of Google Compute Engine resources of the processing pipeline(s). It also provides a monitoring user interface for understanding pipeline health.

### *Cloud Datalab*

Google Cloud Datalab is an interactive tool for exploration, transformation, analysis and visualization of customer's data on Google Cloud Platform. It runs in their cloud project and



enables them to write code to use other Big Data and storage services using a rich set of Google- authored and third party libraries.

### *Cloud Dataproc*

Cloud Dataproc is a fast, easy to use, managed Spark and Hadoop service for distributed data processing. It provides management, integration, and development tools for unlocking the power of rich open source data processing tools. With Cloud Dataproc, users can create Spark/Hadoop clusters sized for their workloads precisely when they need them.

### *Cloud Pub/Sub*

Cloud Pub/Sub is designed to provide reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a “topic” while other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Google Cloud Pub/Sub allows developers to communicate between independently written applications.

### *Genomics*

Genomics provides an Application Programming Interface (API) to store, process, inspect and share DNA sequence reads, reference-based alignments, and variant calls, using Google's cloud infrastructure.

### *App Engine*

App Engine enables developers to build and host web apps on the same systems that power Google applications. App Engine offers fast development and deployment; simple administration with no need to worry about hardware, patches or backups; and effortless scalability. App Engine also provides the ability to create Managed VMs. In addition, developers can build client APIs for their App Engine applications using Google Cloud Endpoints.

### *Cloud Functions*

Cloud Functions is a lightweight, event-based, asynchronous compute solution that allows users to create small, single-purpose functions that respond to cloud events without the need to manage a server or a runtime environment. Events from Google Cloud Storage and Google Cloud Pub/Sub can trigger Cloud Functions asynchronously, or users can use HTTP invocation for synchronous execution.

### *Compute Engine*

Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud. Developers can use Google Compute Engine to solve large-scale processing and analytic problems on Google's computing, storage, and networking infrastructure.

### *Kubernetes Engine*

Kubernetes Engine, powered by the open source container scheduler Kubernetes, enables users to run containers on Google Cloud Platform. Kubernetes Engine takes care of provisioning and maintaining the underlying virtual machine cluster, scaling their application, and operational logistics such as logging, monitoring, and cluster health management.

### *Cloud AutoML Natural Language*

AutoML Natural Language enables customers to categorize input text into their own custom defined labels (supervised classification). Users can customize models to their own domain or use case.

### *Cloud AutoML Translation*

AutoML Translation makes it possible for developers with limited machine learning expertise to train high-quality custom models so translation queries return results specific to their domain. After uploading translated language pairs, AutoML Translation will train a model that can scale as needed to adapt to demands. AutoML Translation offers the ability to create a production-ready model in a short amount of time.

### *Cloud AutoML Vision*

AutoML Vision makes it possible for developers with limited machine learning expertise to train high-quality custom models to classify images according to defined labels. After uploading and labeling images, AutoML Vision will train a model that can scale as needed to adapt to demands. AutoML Vision offers high model accuracy and fast time to create a production-ready model.

### *Cloud Talent Solution*

Cloud Talent Solution brings the power of Google Cloud AI to the talent industry, helping job boards, applicant tracking systems, and recruitment technology vendors provide higher quality job search services to their users, and helping staffing agencies and enterprise hiring companies provide higher quality candidate search capabilities to their recruiters. All of this is made available through a set of APIs, providing access to Google Cloud's AI in the talent space without needing your own machine learning team.

### *Cloud Machine Learning Engine*

Cloud Machine Learning Engine is a managed service that enables users to easily build machine learning models with the powerful TensorFlow framework. It provides scalable training and prediction services that work on large scale datasets.

### *Cloud Natural Language API*

Cloud Natural Language API provides powerful natural language understanding as an easy to use API. This API enables application developers to answer the following questions: 1) What are the entities referred to in the block of text?; 2) What is the sentiment (positive or negative) for this block of text?; 3) What is the language of this block of text?; and 4) What is the syntax for this block of text (including parts of speech and dependency trees)? Users can call this API by passing in a block of text or by referring to a document in Google Cloud Storage.

### *Cloud Speech-to-Text*

Cloud Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy to use API. To support customer global user base, the API can recognize over 80 languages and variants. Users can transcribe the text of users dictating to an application's microphone, enable command-and-control through voice, or transcribe audio files, among many other use cases. Users can stream audio directly to the API or pass URL to audio stored in Google Cloud Storage.

### *Cloud Text-to-Speech*

Google Cloud Text-to-Speech enables developers to synthesize natural-sounding speech with 30 voices, available in multiple languages and variants. It applies DeepMind's research in WaveNet and Google's powerful neural networks to deliver high fidelity audio. With this easy-to-use API, developers can create lifelike interactions with their users, across many applications and devices.

### *Cloud Translation API*

Cloud Translation API automatically translates text from one language to another language (e.g., French to English). Users can use the API to programmatically translate text in their webpages or apps.

### *Cloud Vision API*

Cloud Vision API enables developers to understand the content of an image by encapsulating powerful machine learning models in an easy to use API. It quickly classifies images into thousands of categories (e.g., "sailboat", "lion", "Eiffel Tower"), detects individual objects and faces within images, and finds and reads printed words contained within images. Users can build metadata on their image catalog, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. Users can also analyze images uploaded in the request and integrate with their image storage on Google Cloud Storage.

### *Dialogflow Enterprise Edition*

Dialogflow is a development suite for voice and text conversational apps including chatbots. Dialogflow is cross-platform and can connect to customer's own apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Actions on Google, Facebook Messenger, Slack).

### *Cloud Video Intelligence API*

Cloud Video Intelligence API makes videos searchable, and discoverable, by extracting metadata with an easy to use REST API. It annotates videos stored in Google Cloud Storage, and helps identify key noun entities in a video and when they occur within the video.

### *Cloud SDK*

Cloud SDK is a set of command-line tools for the Google Cloud Platform that can be run interactively or in automated scripts. These tools can be used to manage Compute Engine virtual machines, network and firewall configurations, disk storage, and much more without having to use the Cloud Platform Console.

### *Cloud Source Repositories*

Cloud Source Repositories provides Git version control to support collaborative development of any application or service as well as a source browser that can be used to browse the contents of repositories and view individual files from within the Cloud Console. Cloud Source Repositories and related tools (e.g., Stackdriver Debugger) can be used to view debugging information alongside user's code during application runtime.

### *Cloud Build*

Cloud Build lets developers create container images from application source code located in Google Cloud Storage or in a third party service (e.g., Github, Bitbucket). Created Container images can be stored in Container Registry and deployed on Container Engine, Compute Engine, App Engine Flexible Environment or other services where users can run applications from Docker containers.

### *Container Registry*

Container Registry is a private Docker image storage system on Google Cloud Platform. The registry can be accessed through an HTTPS endpoint, or our own hardware.

### *Cloud Billing API*

Cloud Billing API provides methods such that users can use to programmatically manage billing for their projects on the Google Cloud Platform.



### *Cloud Console*

Cloud Console is used to manage and get insights into everything that powers the cloud application -- including web applications, data analysis, virtual machines, datastore, databases, networking, and developer services. Google Cloud Console helps users to deploy, scale and diagnose production issues in a simple web based interface. Search to quickly find resources and connect to instances via SSH in the browser. Handles devops workflows on the go with powerful native iOS and Android applications.

### *Cloud Deployment Manager*

Deployment Manager is an infrastructure management service that makes it simple to create, deploy, and manage Google Cloud Platform resources.

### *Cloud Console Mobile App*

Cloud Console Mobile App is a native mobile app that enables customers to manage key Google Cloud services. It provides monitoring, alerting, and the ability to take actions on resources.

### *Cloud Shell*

Cloud Shell provides command-line access to Google Cloud Platform resources through an in-browser Linux shell backed by a temporary Linux VM in the cloud. It allows developers to manage their projects and resources without having to install additional tools on their system and comes equipped and configured with common developer tools such as text editors, a MySQL client and kubernetes.

### *GCP Marketplace*

GCP Marketplace is a marketplace that offers ready-to-go development stacks, solutions, and services to accelerate development. It enables users to deploy production-grade solutions in a few clicks, obtain direct access to partner support, and receive a single bill for all GCP and 3rd party services.

### *Stackdriver Debugger*

Stackdriver Debugger enables developers to inspect the call-stack and variables of a running cloud application, in real-time, without stopping or slowing it down. It is safe to use in test, production or any other deployment environment. It can be used to debug applications written in any programming language.

### *Stackdriver Error Reporting*

Stackdriver Error Reporting counts, analyzes and aggregates the crashes in applications. The crash data is extracted from application logs on Google Cloud or reported via the public API.

Users can inspect the collected data via the UI or the public API and may opt-in to receive notifications about the occurrence of errors.

### *Stackdriver Logging*

Stackdriver Logging is a fully-managed service that allows users to store, search, analyze, monitor, and alert of log data and events from Google Cloud Platform and Amazon Web Services (AWS). The API also allows ingestion of any custom log data from any source. Stackdriver Logging can ingest application and system log data from thousands of VMs and analyze log data in real-time.

Software related to Stackdriver Logging (i.e. open-source logging agent) that customers are able to download and install on their own VMs is out of the scope of this report.

### *Stackdriver Profiler*

Stackdriver Profiler continuously gathers and exposes source-level performance information from production services. It allows customers to find out what functions in their code consume the most memory and CPU cycles so that they can gain insight into how their code operates, improve performance, and optimize their computing resources.

### *Stackdriver Trace*

Stackdriver Trace collects latency data from customers' applications and displays it in the Google Cloud Platform Console. It automatically analyzes trace data to generate in-depth performance reports that help surface performance bottlenecks.

### *Cloud Armor*

Cloud Armor provides access control configurations and at-scale defenses against application-aware and multi-vector attacks.

### *Cloud CDN*

Cloud CDN uses Google's globally distributed edge points of presence to cache HTTP(S) load balanced content close to users.

### *Cloud DNS*

Cloud DNS is a high performance, resilient, global, fully managed DNS service that provides a RESTful API to publish and manage DNS records for applications and services.

### *Cloud Router*

Cloud Router is a fully managed and resilient network service that enables GCP and non-GCP customer networks connected by Cloud VPN to auto-discover and auto-update each other. Cloud Router enables this by dynamically sending updates about changes in its GCP network topology and learning about changes in the other non-GCP network using BGP.

### *Cloud VPN*

Cloud VPN securely connects customer's existing network to their Google Cloud Platform network through an IPsec VPN connection. Traffic traveling between the two networks is encrypted by one VPN gateway, then decrypted and authenticated by the other VPN gateway. This protects users' data as it travels over the Internet.

### *Cloud Interconnect*

Google Cloud Interconnect offers enterprise-grade connections to GCP. This solution allows customers to directly connect their on-premises network to their GCP Virtual Private Cloud.

### *Cloud Load Balancing*

Cloud Load Balancing is a distributed, software-defined, managed service for all traffic (HTTP(S), TCP/SSL, and UDP) to users' computing resources. It is not an instance or device based solution, so users aren't locked into a physical load balancing infrastructure or face the HA, scale and management challenges inherent in instance based load balancers. In contrast to DNS-based Global Load Balancing solutions, Cloud Load Balancing reacts instantaneously to changes in users, traffic, network, backend health and other related conditions.

### *Virtual Private Cloud (VPC)*

Virtual Private Cloud is a comprehensive set of managed networking capabilities including granular IP address range selection, routes and firewalls.

### *Data Loss Prevention API*

Data Loss Prevention (DLP) API helps developers classify and redact content in text, images, and cloud assets using a set of predefined detectors for types of sensitive or personally identifiable information. It quickly classifies text into information types (e.g., phone\_number, social\_security\_number, passport\_number) along with metadata like offsets or bounding boxes for images. Users can use this API in their own workflows and applications to help better understand and manage their data.

### *Cloud Identity and Access Management*

Cloud Identity and Access Management (IAM) lets administrators authorize who can take action on specific resources, giving them full control and visibility to manage access to cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups and potentially many more projects, Cloud IAM provides a unified view into security policy across users entire organization, built-in auditing to ease compliance processes.

### *Cloud Key Management Service*

Cloud Key Management Service (KMS) is a cloud-hosted key management service that lets users manage encryption for their cloud services the same way for on-premise. Users can generate, use, rotate and destroy AES256 (Advanced Encryption Standard) encryption keys.

### *Cloud HSM*

Cloud HSM is a cloud-hosted Hardware Security Module (HSM) service that allows customers to host encryption keys and perform cryptographic operations.

### *Cloud Resource Manager*

Cloud Resource Manager API allows users to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allows users to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization lets users easily manage common aspects of resources such as access control and configuration settings.

### *Cloud Security Scanner*

Cloud Security Scanner is a web application security scanner for Google App Engine. It enables developers to easily check for a subset of common web application vulnerabilities in websites built on App Engine.

### *Cloud Bigtable*

Cloud Bigtable is a fast, fully managed, highly-scalable NoSQL database service. It is designed for the collection and retention of data from 1TB to hundreds of PB.

### *Cloud Datastore*

Cloud Datastore is a fully managed, schemaless, non-relational datastore. It provides a rich set of query capabilities, supports atomic transactions, and automatically scales up and down in response to load. It can scale to support an application with 1,000 users or 10 million users with no code changes.

### *Cloud Firestore*

Cloud Firestore is a flexible, scalable database for mobile, web, and server development from Firebase and Google Cloud Platform. Like Firebase Realtime Database, it keeps customer's data in sync across client apps through realtime listeners and offers offline support for mobile and web so they can build responsive apps.

### *Cloud Memorystore*

Cloud Memorystore for Redis provides a fully managed in-memory data store service built on scalable, more secure, and highly available infrastructure managed by Google. Developers can

use Cloud Memorystore to build application caches that provides sub-millisecond data access. Cloud Memorystore is compatible with the Redis protocol, allowing easy migration with zero code changes.

### *Cloud Spanner*

Cloud Spanner is a fully managed, mission-critical relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and strong consistency at global scale.

### *Cloud SQL*

Cloud SQL is a web service that allows developers to create, configure, and use relational databases that live in Google's cloud. It is a fully-managed service that maintains, manages, and administers databases, allowing users to focus on their applications and services.

### *Cloud Storage*

Cloud Storage is a RESTful service for storing and accessing data on Google's infrastructure. The service combines the performance and scalability of Google's cloud with advanced security and sharing capabilities.

### *Cloud Storage Transfer Service*

Cloud Storage Transfer Service enables customers to import large amounts of online data into Google Cloud Storage. With Storage Transfer Service, customers can transfer data from Amazon Simple Storage Service (Amazon S3) and other HTTP/HTTPS locations as well as transfer data between Google Cloud Storage buckets.

### *Persistent Disk*

Persistent Disk provides a persistent virtual disk for use with Google Compute Engine and Google Kubernetes Engine compute instances. It is available in both SSD (Solid State Drive) and HDD (Hard Disk Drive) variations.

### *Cloud Endpoints*

Google Cloud Endpoints is a tool that helps customers to develop, deploy, secure and monitor their APIs running on Google Cloud Platform.

### *Cloud Healthcare API*

Cloud Healthcare API provides managed services and an API to store, process, manage, and retrieve healthcare data in a variety of industry standard formats including HL7, FHIR, and DICOM.

### *Cloud Identity-Aware Proxy*

Cloud Identity-Aware Proxy (Cloud IAP) is a tool that helps control access to a user's applications running on Google Cloud Platform based on a user's identity and group membership.

### *Cloud IoT Core*

Cloud IoT Core is a fully managed service that allows customers to securely connect, manage, and ingest data from millions of globally dispersed devices. Cloud IoT Core, in combination with other services on Google Cloud IoT platform, provides solutions for collecting, processing, analyzing, and visualizing IoT data in real time to support improved operational efficiency.

### *Google Service Control*

Google Service Control provides control plane functionality to managed services, such as logging, monitoring, and status checks.

### *Orbitera*

Orbitera provides a platform which allows enterprise customers to create time-bound multi-cloud software trials; import billing data and generate reports and invoices; and create marketplaces to sell solutions.

### *Service Consumer Management API*

Service Consumer Management API provides utilities to help managed service producers manage their relationships with their services' consumers, including the ability to create and manage tenancy units.

### *Service Management API*

Service Management API provides methods for publishing managed services and managing service configurations.

## **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.