Using Google Cloud in the Context of NCSC UK's Cloud Security Principles

July 2017

Table of Contents

This document is provided for informational purposes only and is not legal advice. We encourage you to obtain appropriate guidance for your particular use of GCP and the compliance, legal and regulatory requirements that apply to you. Service information is subject to change. Please visit https://cloud.google.com/ for the most current information.

Introduction

Terminology / User Types

Role	Description
Google	The Cloud Service Provider
Admin	An individual managing G Suite and/or Google Cloud Platform admin services
End User	This term applies to G Suite only and is used to refer to the users a G Suite Admin manages
Customer	An individual provided access to the services and whose data is managed by the Admin

1. Data in Transit Protection

Security Principle (link)	Confirmation
Data in transit is protected between the consumer's end user devices and the service.	G Suite and Google Cloud Platform meet objective
Data in transit is protected internally within the service.	G Suite and Google Cloud Platform meet objective
Data in transit is protected between the service and other services (e.g. where APIs are exposed).	G Suite and Google Cloud Platform meet objective

Customer information is encrypted while it's en route from one machine to another, protecting these data transmissions should they be intercepted. Data in transit may be traveling in one of the four ways described below. In each case, Google's network protection and encryption measures are outlined.

1.1 Over the Internet

When a customer uses a Google service, their information travels over the Internet between their browser, Google's servers, and any non-Google users they are communicating with. In these scenarios, encryption prevents hackers from exploiting vulnerabilities in Internet connections to steal login credentials, eavesdrop on emails, or collect other sensitive data. Industry-standard firewalls and access control lists (ACLs) are used to enforce network segregation. All traffic is routed through custom GFE (Google Front End) servers to detect and stop malicious requests and Distributed Denial of Service (DDoS) attacks. Additionally, GFE servers are only allowed to communicate with a controlled list of servers internally; this "default deny" configuration prevents GFE servers from accessing unintended resources. Logs are routinely examined to reveal any exploitation of programming errors.

1.2 Between the Customer and Google

To protect customer information, the first step is having a secure browser that supports the latest encryption and security updates. For Google customers (G Suite or Google Cloud Platform), we automatically encrypt traffic between their browser and our data centers. This encryption happens whether they are using public WiFi, logging in at the office, or working from home on their computer, phone or tablet.

Google websites and properties use the following robust public key technologies: 2048-bit RSA or P-256 ECDSA SSL certificates issued by a trusted authority (currently the Google Internet Authority G2). The encryption works differently depending on the the customer's client configuration as this depends on the customer's system, and browser version; for example, Google still supports TLS 1.0 and SHA1 and MD5 hashes for encryption. The browser will always negotiate the highest mutually implemented versions.

Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA ("ECDHE_RSA" and "ECDHE_ECDSA"; see Table 1 for details). These are referred to as 'forward secrecy methods' and help protect any traffic between the customer and Google servers from being intercepted and decrypted by man-in-the-middle (MitM) attacks. In 2011, we announced forward secrecy by default.

Forward secrecy technology helps ensure that information encrypted today is less vulnerable to new methods of breaking encryption in the future. With forward secrecy, keys are rotated at least every other day as opposed several months with other methods. Doing so limits the window of potentially decryptable customer information from a compromised encryption key. Without forward secrecy, an adversary could record encrypted traffic and store it with the hope of compromising the HTTPS private key at a later date. With forward secrecy, Google servers generate a new Diffie-Hellman public key for each session, sign the public key, and use Diffie-Hellman to generate mutual private keys with the customer's browser. This helps prevent eavesdropping as every session between a customer and Google is encrypted using different public keys. To fully decrypt the data, an attacker would have to capture encrypted traffic *and* compromise the temporary private key before it's destroyed.

Protocols	Cipher Suites	Signing Keys	Hash Functions
TLS 1.3	ECDHE_RSA with AES	RSA 2048	SHA384
TLS 1.2	ECDHE_RSA with 3DES	ECDSA P-256	SHA256
TLS 1.1	ECDHE_ECDSA		SHA1
TLS 1.0	RSA with AES		MD5
QUIC	RSA with 3DES		

Table 1 - Encryption Protocols and Ciphers supported for data in transit between the customer and Google

1.3 Between the Customer and Non-Google Users

Google implements HTTPS Transport Layer Security (TLS) version 1.2 by default, enhanced by Perfect Forward Secrecy. The two sections below outline how G Suite and the Google Cloud Platform (GCP) handle data transit to non-Google users.

1.3.1 G Suite

Google has led the industry in using TLS for email routing. This allows Google and non-Google servers to communicate in an encrypted manner. When a G Suite end user sends an email from Google server to a non-Google server that participates in TLS, they are protected. G Suite end users can use the product to restrict email communication to domains and addresses covered by TLS. This restriction can be managed through the TLS compliance setting.

1.3.2 Google Cloud Platform

Google provides services and features that enable GCP admins to secure their interactions with their customers via HTTPS.

1.4 Between Data Centers

A key security advantage for Google customers is its vast and robust network of data centers that spans the globe. The network is designed to minimize latency and maximize availability, helping our customers have uninterrupted access to their data. The connections between internal Google Servers are cryptographically authenticated. Certain connections (including those to and from the Key Management Service (KMS)) are encrypted with a TLS-like proprietary transport protocol that uses AES 128-bit or higher. This internal movement of data is imperceptible to our customers.

Both GCP and G Suite rely on API interactions. Access to these APIs are protected by the OAuth-key. Each application has to authenticate in order to get access to the service. In addition to authentication, access to these APIs is SSL-protected. More information on API access can be found in Using OAuth 2.0 to Access Google APIs.

1.4.1 G Suite

G Suite uses an encrypted HTTPS connection when an end user logs in and uses the service. Google has supported HTTPS since it launched and in 2010 we made HTTPS the default.

1.4.2 Google Cloud Platform

GCP resources can be created and deployed across multiple regions and zones. In GCP, the admin can choose where they want certain data stored. A full list of our GCP data centers can be found on our Cloud Locations Map.

Additional information can be found in the SOC 2 report, under the "Availability Principle and Criteria" section. Contact your Google account representative for more.

2. Asset Protection and Resilience

2.1 Physical Location and Legal Jurisdiction

Security Principle (link)	Confirmation
The geographic location(s) where consumer data is stored, processed or managed from (to country level)(principle).	G Suite and GCP meet the objective: ● G Suite Data Center Locations ● GCP Data Center Locations
The applicable legal jurisdiction(s) that the service provider operates within.	Google is a global technology service provider

Google is a global technology service provider. To learn more about our data centers please see here for G Suite and here for GCP.

The European Union's Data Protection Authorities have confirmed that Google Cloud services' contractual commitments fully meet the requirements for data transfers outside of the EU, in accordance with EU Data Protection Directive 95/46/EC. This compliance finding enables customers in most EU countries to rely on GCP and G Suite model contract clauses for the international transfer of data without further authorizations. Please see here for more and see Section 4 of this document for more regarding compliance.

2.2 Data Center Security

Security Principle (link)	Confirmation
Access to those locations within the service that allow access to consumer data is protected.	G Suite and GCP meet the objective.

Google's focus on the security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and the data center floor features a laser beam intrusion detection system. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Our data centers are routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Access to the data center floor is only possible via a security corridor which implements multi factor access control using both security badges and biometrics. Only approved employees with specific roles may enter.

Google's data centers are geographically distributed and employ a variety of physical security measures. The technology and security mechanisms used in these facilities may vary depending on local conditions such as building location and regional risks. The standard physical security controls implemented at each Google data center are composed of well-known technologies and follow generally accepted industry best practices. Some examples of these practices include custom designed electronic card access control systems, alarm systems, interior and exterior cameras, and security guards. Access to areas where systems, or system components, are installed or stored are segregated from general office and public areas such as lobbies. The cameras and alarms for each of these areas are centrally monitored for suspicious activity, and the facilities are routinely patrolled by security guards who use bicycles, Segways and T3 motion scooters.

Google's facilities use high resolution cameras with video analytics and other systems to detect and track intruders. Activity records and camera footage are kept for later review, if needed. Additional security controls such as thermal imaging cameras, perimeter fences and biometrics are used when necessary.

Access to all data center facilities is restricted to authorized Google employees, approved visitors, and approved third parties whose job it is to operate the data center. Google maintains a visitor access policy mandating that a data center manager approve any visitors in advance and only for the specific internal areas they are visiting. This policy also applies to Google employees who do not normally have access to data center facilities. Google audits who has access to its data centers on a quarterly basis to help ensure that only appropriate personnel have access to each floor.

Google restricts access to its data centers based on role, not position. As a result, even the most senior executives at Google do not have access to Google data centers. Less than one percent of Googlers will ever step foot in one of our data centers.

Additional information can be found in the SOC 2 report, under the "Physical Access - Data Center Physical Security" section. Contact your Google account representative for more.

2.3 Data at Rest Protection

Security Principle (link)	Confirmation
Storage media containing consumer data is protected from unauthorised access - this includes removable and fixed storage media.	G Suite and GCP meet the objective: ● ISO/IEC 27001 certification achieved. ● ISO/IEC 27017 certification achieved. ● SOC 2 report available.

2.3.1 Overview

Central to our comprehensive security strategy is encryption of data at rest which ensures that data can be accessed only by the authorized roles and services with audited access to the encryption keys. This section describes the encryption and key management processes we have in place to secure data at rest.

2.3.2 Layers of Encryption

Google uses several layers of encryption to protect data. Using multiple layers of encryption adds redundant data protection and allows Google to select the optimal approach based on application requirements.

Figure 1 below shows the layers of encryption used in both G Suite and GCP infrastructures.

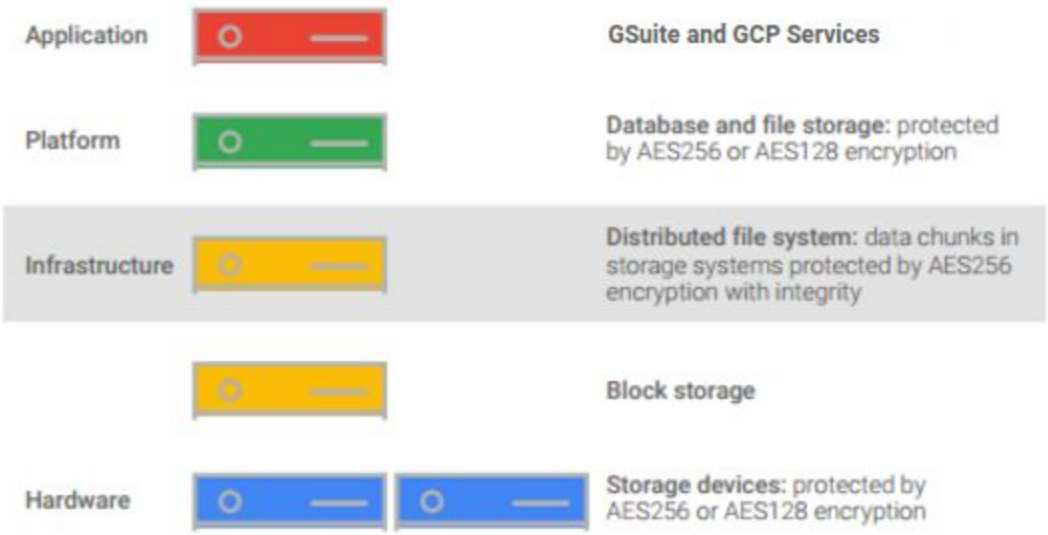

Figure 1 - Layers of Encryption

2.3.3 Encryption at the Storage System Layer

Customer data is broken into subfile chunks for storage; each chunk can be up to several GB in size. Each chunk is encrypted at the storage level with an individual encryption key: no two chunks will have the same key, even if they are owned by the same customer or stored on the same machine. If a chunk of data is updated, it is encrypted with a new key rather than reusing an existing key. This partition of data, each using a different key, means the “blast radius” of a potential data encryption key compromise is limited to only that data chunk.

Google encrypts data prior to it being written to disk. Encryption is inherent in all of Google’s storage systems, rather than being added afterwards.

Each data chunk has a unique identifier. Access Control Lists (ACLs) ensure that each chunk can be decrypted by only Google services operating under authorized roles, which are granted access at that point in time. This prevents access to the data without authorization, bolstering both data security and privacy.

Figure 2 below shows how data at Google is broken up into encrypted chunks for storage.

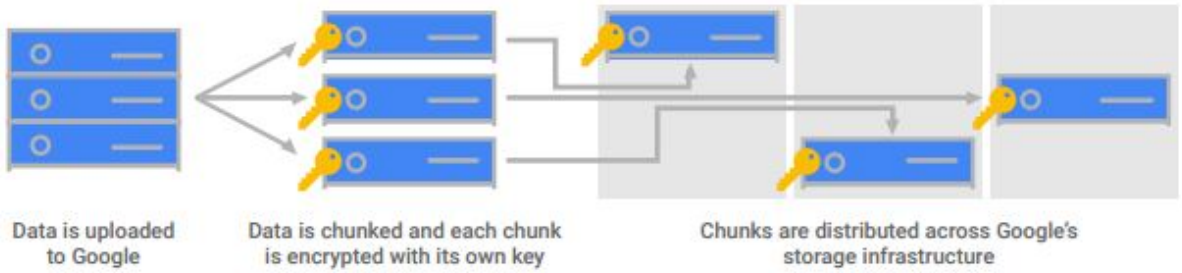

Figure 2 - Data Chunking at Google

Each chunk is distributed across Google's storage systems, and is replicated in encrypted form for backup and disaster recovery. A malicious individual who wanted to access customer data would need to know and be able to access all storage chunks corresponding to the data they want and the encryption keys corresponding to the the chunks.

2.3.4 Encryption at the Storage Device Layer

In addition to the storage system level encryption described above, in most cases data is also encrypted at the storage device level, with at least AES128 for hard disks (HDD) and AES256 for new solid state drives (SSD), using a separate device-level key (which is different than the key used to encrypt the data at the storage level). As older devices are replaced, solely AES256 will be used for device-level encryption.

2.3.5 Key Management

Managing keys safely and reliably, while allowing access to the keys only to authorized services and individuals, is central to encrypted data security. Google has built a robust proprietary service for the distribution, generation, rotation and management of cryptographic keys using industry standard cryptographic algorithms that are in alignment with stronger industry practices. In the following sections, we'll outline our approach to managing the encryption keys used to protect customer information.

2.3.5.1 Google's Internal Key Management Service (KMS)

As described in section 2.3.3, files or data structures with customer related content written by Google are subdivided into chunks. The key used to encrypt the data in a chuck is called a data encryption key (DEK). The DEKs are encrypted with (or "wrapped" by) a key encryption key (KEK). These KEKs are stored centrally in Google's Key Management Service (KMS), a repository built specifically for storing keys.

For each Google customer, any non-shared resources [1] are split into data chunks and encrypted with keys separate from keys used for other customers [2]. These DEKs are even separate from those that protect other pieces of the same data owned by the same customer.

DEKs are generated by the storage system using Google's common cryptographic library. They are then sent to KMS to wrap with that storage system's KEK, and the wrapped DEKs are passed back to the storage system to be kept with the data chunks. When a storage system needs to retrieve encrypted data, it retrieves the wrapped DEK and passes it to the KMS. The KMS then verifies that this service is authorized to use the KEK, and if so, unwraps and returns the plaintext DEK to the service. The service then uses the DEK to decrypt the data chunk into plaintext and verify its integrity.

Most KEKs for encrypting data chunks are generated within the KMS, and the rest are generated inside the storage services. For consistency, all KEKs are generated using Google's common cryptographic library, using a random number generator (RNG) built by Google.

Google's KMS manages KEKs, and was built solely for this purpose. It was designed with security in mind. KEKs are not exportable from Google's KMS by design; all encryption and decryption with these keys must be done within KMS. This helps prevent leaks and misuse, and enables KMS to emit an audit trail when keys are used.

2.3.5.2 Rotating Keys to Limit Risk

Google's internal KMS can automatically rotate KEKs at regular time intervals. Though we often refer to just a single key, we really mean that data is protected using a key set: one key active for encryption and a set of historical keys for decryption, the number of which is determined by the *key rotation schedule*. The actual rotation schedule for a KEK varies by service. For example, Google Cloud Storage rotates its KEKs every 90 days, and can store up to 20 versions, requiring re-encryption of data at least once every 5 years (though in practice, data re-encryption is much more frequent). As mentioned earlier, DEKs are not rotated, but rather a new DEK is generated whenever data is written.

2.3.5.3 Auditing and Access Control for Keys

The use of KEKs is managed by access control lists (ACLs) in KMS for each key, with a per-key policy. Only authorized Google services and users are allowed access to a key. The use of each key is tracked at the level of individual operation that requires that key - so every time an

[1] An example of a shared resource (where this segregation does not apply) would be a shared base image in Google Compute Engine — naturally, multiple customers refer to a single copy, which is encrypted by a single DEK.
[2] With the exception of data stored in Cloud Datastore, App Engine, and Cloud Pub/Sub, where more than one customer's data may be encrypted with the same DEK.

individual uses a key, it is authenticated and logged. All human data accesses are auditable as part of Google's overall security and privacy policies.

For more information on the encryption used at Google, see the Encryption at Rest whitepaper. For information on the core content and granularity of encryption in each service, see the G Suite encryption whitepaper, and the Google Cloud Platform encryption whitepaper.

2.4 Data Sanitation

Security Principle (link)	Confirmation
Service providers inform customers of how long it will be before consumer data (and any backups) is securely sanitised following the termination of the contract or exit from the service.	G Suite and GCP meet the objective. Once a Customer or End User deletes Customer data (and such Customer data cannot be recovered by the Customer or End User) Google will delete such data from its systems as soon as is reasonably practicable and within a maximum period of 180 days.
Service providers securely erase consumer data when resources are moved reprovisioned, when the consumer leaves the service and upon request by the consumer.	G Suite and GCP meet the objective: ● ISO/IEC 27001 certification achieved. ● ISO/IEC 27017 certification achieved. ● SOC 2 report available.
Storage media which has held consumer data is sanitised or securely destroyed at the end of usable lifetime.	G Suite and Cloud meet the objective: ● ISO/IEC 27001 certification achieved. ● ISO/IEC 27017 certification achieved. ● SOC 2 report available - the process conforms to NIST 800-88

2.5 Equipment Disposal

Security Principle (link)	Confirmation
All equipment potentially containing consumer data, credentials, or configuration information for the service is identified at the end of its life or prior to being recycled.	G Suite and GCP meet the objective: ● ISO/IEC 27001 certification achieved. ● ISO/IEC 27017 certification achieved. ● SOC 2 Report Available.
Any components containing sensitive data are sanitized, removed or destroyed as appropriate.	G Suite and GCP meet the objective: ● ISO/IEC 27001 certification achieved. ● ISO/IEC 27017 certification achieved. ● SOC 2 Report Available.
Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.	G Suite and GCP meet the objective: ● ISO/IEC 27001 certification achieved. ● ISO/IEC 27017 certification achieved. ● SOC 2 Report Available - the process conforms to NIST 800-88

Google has strict policies and procedures that govern the management of the equipment lifecycle within its production data centers. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorized by appropriate operations manager before release.

2.6 Physical Resilience and Availability

Security Principle (link)	Confirmation
Services have varying levels of resilience, which will affect their ability to operate	G Suite and GCP meet the objective.

normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, with attendant business impacts

Overview

As part of our contract with our customers, we agree to maintain a certain level service availability and resilience. The sections below provide further details on this agreement for both G Suite and GCP.

G Suite

During the term of the applicable G Suite Agreement, the G Suite Covered Services web interface will be operational and available to the customer at least 99.9% of the time in any calendar month. If Google does not meet its G Suite SLA and the customer meets its obligations under the same SLA, the customer is eligible to receive service credits. The SLA states that service credits are the customer's sole and exclusive remedy for any failure by Google to meet the Google Suite SLA.

Google Cloud Platform

The Cloud console itself has no SLA, however, the platform services do. Individual services have their own SLA and conditions as part of our engagement with the customer. For more information on platform service SLA's, see the Google Cloud Platform Service Level Agreements.

Additional information can be found in the SOC 2 report, under the "Availability Principle and Criteria" section. Contact your Google account representative for more.

2.7 EU Data Protection Implications

The EU Data Protection Directive is an important piece of privacy legislation passed by the European Union (EU) in 1995. It restricts the movement of data from the EU to non-EU countries that do not meet the EU 'adequacy' standard for privacy protection. In 2010, the European Commission approved model contract clauses as a means of compliance with the requirements of the Directive. The effect of this decision is that by incorporating certain provisions into a contract, personal data can flow from those subject to the directive to providers outside the EU or the European Economic Area. Google offers Model Contract Clauses as an additional means

of meeting the adequacy and security requirements of the European Commission's Data Protection Directive for our customers who operate within Europe.

The European Union's data protection authorities have concluded that Google's model contract clauses meet EU regulatory expectations, confirming that Google Cloud services provide sufficient commitments to frame international data flows from Europe to the rest of the world. For details on the approval of the Google Cloud from the Article 29 Working Party, please see the respective decisions for G Suite and the Google Cloud Platform and Google's public statement.

For further information on EU data protection implications, see the following links:

- G Suite Data Processing Amendment
- G Suite EU Model Contract Clauses
- G Suite Common Opinion Application
- G Suite Implementation Instructions
- GCP Data Processing and Security Terms
- GCP EU Model Contract Clauses
- GCP Common Opinion Application
- GCP Implementation Instructions

3. Separation Between Consumers

Security Principle (link)	Confirmation
Service providers make available the following information to consumers: ● The consumers that the service is shared with. This should include whether the service is a public, private or community cloud service. For community cloud services, the groups which the community includes should be specified. ● The connectivity requirements or terms and conditions the consumers are bound by ● How consumers are separated within the service	G Suite meets this objective: ● G Suite for Business is a public cloud service ● Recommendations are available ● G Suite Encryption Whitepaper
Separation between consumers of the service prevents one consumer affecting the	G Suite and GCP meet this objective

confidentiality or integrity of another consumers data or service. For IaaS, separation is enforced across the service, including at the compute, storage and networking layers.	GCP meets this objective. See the Google Infrastructure Design Overview.
For PaaS and SaaS, separation between consumers is enforced at all points within the service, where the service is exposed to consumers.	G Suite and GCP meet this objective
Separation within the consumer service management interface is also an important consideration. This is covered separately as part of Principle 9.	G Suite and GCP meet this objective

3.1 Within Google's Infrastructure

Google has extensive controls and practices to protect the security of customer information.

Google applications run in a multi-tenant, distributed environment. Rather than segregating each customer's data onto a single machine or set of machines, Google Cloud data from all Google customers (end users, business, and even Google's own data) is distributed amongst a shared infrastructure composed of Google's many homogeneous machines and located across Google's many data centers

Data is broken into subfile "chunks," which are stored on local disks and identified by unique chunk IDs. Google encrypts data as it is written to disk with a per-chunk encryption key that is associated with a specific Access Control List (ACL). The ACL helps ensure that data in each chunk is only decrypted by authorized Google employees and services that were given permission at the time of encrypting the data. This means that different chunks are encrypted with different encryption keys, even if they belong to the same customer. These chunks are encrypted using 128-bit or stronger Advanced Encryption Standard (AES).

3.2 Key Management and the Decryption Process

Managing keys safely and reliably, while allowing access to the keys only to authorized services and individuals, is central to encrypted data security. Google has built a robust proprietary service for the distribution, generation, rotation and management of cryptographic keys using industry standard cryptographic algorithms that are in alignment with strong industry security practices. In the following sections, we'll outline our approach to managing the encryption keys used to protect Google customer's' information.

As described in section 2.3.3, files or data structures with customer created content written by Google are subdivided into chunks, each of which is encrypted with its own chunk data encryption key (the "chunk key"). Each chunk key is encrypted by another key known as the wrapping key, which is managed by a Google-wide Key Management Service (KMS). The result is a "wrapped" (encrypted) chunk key, which is stored alongside the encrypted data. The wrapping keys, needed to decrypt wrapped chunk keys, and therefore to decrypt the chunk, are known only to the KMS and are never stored at rest in unencrypted form. Decryption and encryption operations on chunk keys are performed within the KMS. The wrapped chunk key is sent by a storage system to the KMS as a request to be unwrapped (decrypted) in order to access the encrypted data. The KMS authenticates the requesting system and checks the request against both system-level and per-wrapped-key ACLs. If this request is authorized, the chunk data key is decrypted in the KMS and returned to the storage system, which can now use that chunk key to decrypt that specific chunk of data. These chunk keys are encrypted in transit, as described in figure 5 below. This process is repeated until all the chunks that compose a specific file or data structure are decrypted, making the data available to the requesting application.

Data cannot be decrypted without both the wrapping key and the wrapped chunk key. Decrypting data therefore requires the cooperation of the storage system (which holds the encrypted data and wrapped chunk key) and the KMS (which holds the wrapping key). The KMS wrapping keys that encrypt the chunk keys are 128-bit or stronger AES keys. All access to the KMS is controlled by ACLs.

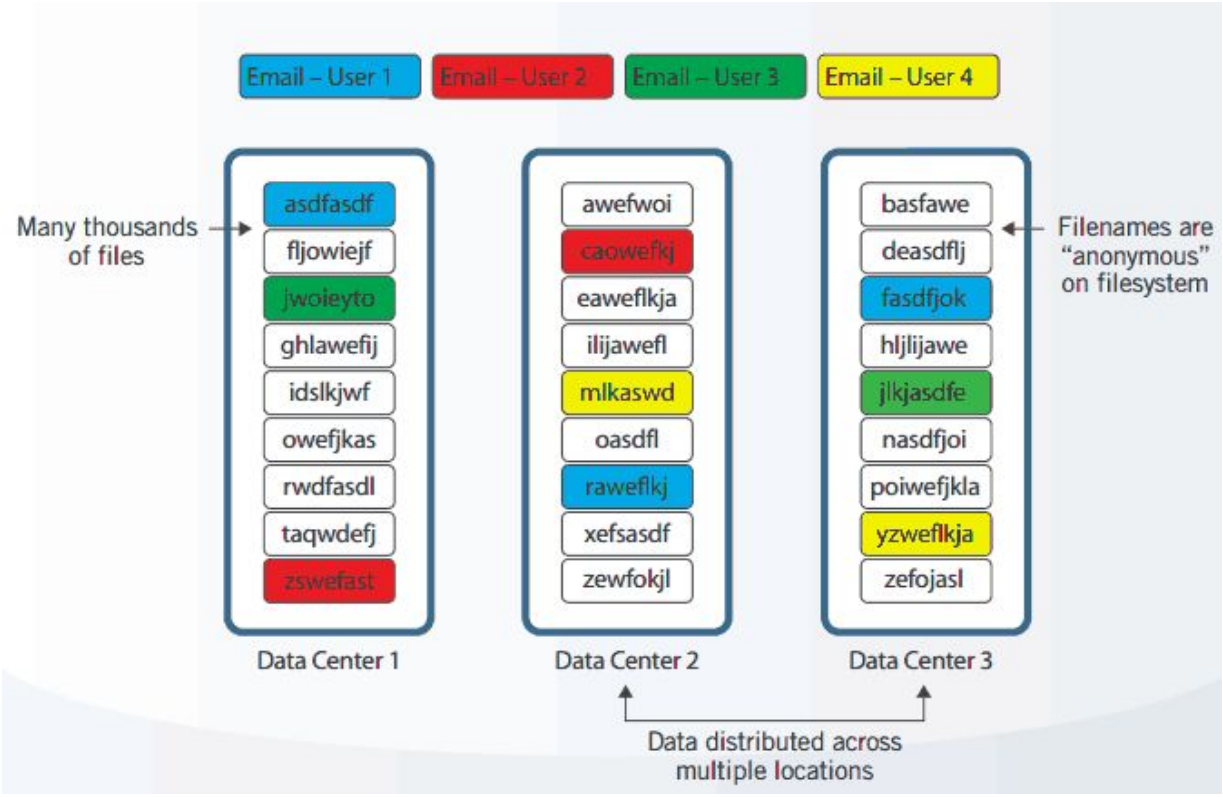

Figure 5 - Customer Data at Rest

The layers of the Google application and storage stack require that requests coming from other components are authenticated and authorized. Service-to-service authentication is based on a security protocol that relies on a Google system to broker authenticated channels between application services. In turn, trust between instances of this authentication broker is derived from x509 host certificates that are issued to each Google production host by a Google-internal certificate authority.

3.3 Customer Separation in G Suite

Access to end-user data is restricted, with only the end-user having access to their own data, unless they explicitly share it. Google does not permit access to customer data by administrators from the G Suite admin panel.

For more information on encryption and key management, see the G Suite Security Whitepaper and the GCP Security Whitepaper.

4. Governance

Security Principle (link)	Confirmation
The service provider has a clearly identified, and named, board representative (or a person with the direct delegated authority of) who is responsible for the security of the Cloud service. This is typically someone with the title of Chief Security Officer, Chief Information Officer, or Chief Technical Officer.	G Suite and GCP meet this objective.
The service provider's security governance framework is formally documented, as are policies governing key aspects of information security relating to the service.	G Suite and GCP meet this objective.
Information security is incorporated into the service provider's financial and operational risk reporting mechanisms for the service	G Suite and GCP meet this objective.
The service provider has processes in place to identify and ensure compliance with applicable legal and regulatory requirements relating to the service.	G Suite and GCP meet this objective.

4.1 Overview

This section covers Google's compliance and certification with three ISO standards. Our compliance with these ISO standards was certified by Ernst & Young CertifyPoint, an ISO certification body accredited by the Dutch Accreditation Council, a member of the International Accreditation Forum (IAF). Certificates issued by Ernst & Young CertifyPoint are recognized as valid certificates in all countries with an IAF member. Read more about GCP and G Suite compliance certifications.

4.2 ISO 27001:2013 Certification

ISO 27001 is one of the most widely recognized and internationally accepted independent security standards. Google has earned ISO 27001 certification for the systems, applications, people, technology, processes and data centers serving G Suite and GCP. More details of the certification can be found in the table below.

	G Suite	Cloud
Auditors	Ernst & Young CertifyPoint	Ernst & Young CertifyPoint
Services Covered	G Suite G Suite (Google Apps Unlimited) G Suite for Education	Google Cloud Platform
Products	Admin Console	App Engine
	App Maker	App Engine Flexible Environment
	Apps Script	BigQuery
	Calendar	Cloud Bigtable
	Chrome Device Management	Cloud Billing API
	Chrome Sync	Cloud CDN (Content Delivery Network)
	Classic Sites	Cloud Console
	Classroom (only G Suite for Education)	Cloud Data Loss Prevention API
	Cloud Identity	Cloud Dataflow
	Cloud Search	Cloud Datalab
	Contacts	Cloud Dataproc
	Docs	Cloud Datastore
	Drive	Cloud DNS (Domain Name System)
	Forms	Cloud Endpoints
	Gmail	Cloud Functions

Google+

Google Now

Google Translate

Groups

Hangouts

Hangouts Chat

Hangouts Meet

Inbox by Gmail

Jamboard

Keep

Sheets

Sites

Slides

Talk

Tasks

Vault

Cloud IAM (Identity & Access Management)

Cloud Jobs API

Cloud Key Management Service

Cloud Launcher

Cloud Load Balancing

Cloud Machine Learning Engine

Cloud Mobile App

Cloud Natural Language API

Cloud Pub/Sub

Cloud Resource Manager

Cloud Router

Cloud SDK

Cloud Security Scanner

Cloud Shell

Cloud Source Repositories

Cloud Speech API

Cloud SQL

Cloud Storage

Cloud Translation API

Cloud Virtual Network

Cloud Vision API

Cloud VPN

Compute Engine

Container Builder

		Container Engine
		Container Registry
		Debugger
		Deployment Manager
		Error Reporting
		Genomics
		Google Service Control
		Jibe Cloud and Hub
		Stackdriver Logging
		Trace
Product APIs	Apps Activity API	
	Calendar API	
	Contacts API	
	Drive REST API	
	Gmail REST API	
	Sheets API	
	Sites API	
	Tasks API	
Admin SDK APIs	Admin Settings API	
	Calendar Resource API	
	Directory API	
	Domain Shared Contacts API	
	Email Audit API	

Email Settings API

Enterprise Licence Manager API

Groups Migration API

Groups Settings API

Reports API

Reseller API

SAML-based SSO API

Common Infrastructure

Data Centers

Atlanta (1)(GA), United States of America

Atlanta (2) (GA), United States of America

Changhua, Taiwan

Council Bluffs (1) (IA), United States of America

Council Bluffs (2) (IA), United States of America

The Dalles (OR), United States of America

Dublin, Ireland

Eemshaven, Groningen, Netherlands

Ghlin, Hainaut, Belgium

Hamina, Finland

Lenoir (NC), United States of

Offices

Mountain View (CA), United States of America

Sunnyvale (CA), United States of America

San Francisco (CA), United States of America

Irvine (CA), United States of America

Boulder (CO), United States of America

Cambridge (MA), United States of America

New York (NY), United States of America

Kirkland (WA), United States of America

Seattle (WA), United States of America

Sydney, Australia

Belo Horizonte, Brazil

America	
Longtan, Taoyuan, Taiwan	Hyderabad, India
Moncks Corner (SC), United States of America	Bangalore, India
Pryor Creek (OK), United States of America	Dublin, Ireland
Quilicura, Santiago, Chile	Tokyo, Japan
Wenya, Singapore	Krakow, Poland
Koto-ku, Tokyo, Japan	Zurich, Switzerland
Ashburn (VA), United States of America	London, United Kingdom
	Waterloo, Ontario, Canada
	Los Angeles (CA), United States of America
	Shanghai, China
	Manila, Philippines
	Gurgaon, India
	San Bruno (CA), United States of America
	Madison (WI), United States of America
	Aarhus, Denmark
	Singapore, Singapore

Table 4 - ISO 27001:2013 Certification

4.3 ISO 27017:2015 Certification

ISO 27017 builds on the well-known standard of ISO 27001 by providing additional controls that address some of the security risks that are more specific to cloud services, ensuring that:

- the security roles and responsibilities between Google and our customers are clearly-defined
- our customers' data may be protected from unauthorized parties and is segregated between different cloud customers
- the security policies for Google's virtual networks are as secure as on our physical networks
- our customers have adequate tools to monitor how their data is handled at Google.

More details of the certification can be found in the table below.

	G Suite	Cloud
Auditors	Ernst & Young CertifyPoint	Ernst & Young CertifyPoint
Services Covered	G Suite	Google Cloud Platform
	G Suite (Google Apps Unlimited)	
	G Suite for Education	
Products	Admin Console	App Engine
	App Maker	App Engine Flexible Environment
	Apps Script	BigQuery
	Calendar	Cloud Bigtable
	Chrome Device Management	Cloud Billing API
	Chrome Sync	Cloud CDN (Content Delivery Network)
	Classic Sites	Cloud Console
	Classroom (only G Suite for Education)	Cloud Data Loss Prevention API
	Cloud Identity	Cloud Dataflow
	Cloud Search	Cloud Datalab
	Contacts	Cloud Dataproc

Docs

Drive

Forms

Gmail

Google+

Google Now

Groups

Hangouts

Hangouts Chat

Hangouts Meet

Inbox by Gmail

Jamboard

Keep

Sheets

Sites

Slides

Talk

Tasks

Vault

Cloud Datastore

Cloud DNS (Domain Name System)

Cloud Endpoints

Cloud Functions

Cloud IAM (Identity & Access Management)

Cloud Jobs API

Cloud Key Management Service

Cloud Launcher

Cloud Load Balancing

Cloud Machine Learning Engine

Cloud Mobile App

Cloud Natural Language API

Cloud Pub/Sub

Cloud Resource Manager

Cloud Router

Cloud SDK

Cloud Security Scanner

Cloud Shell

Cloud Source Repositories

Cloud Speech API

Cloud SQL

Cloud Storage

Cloud Translation API

Cloud Virtual Network

		Cloud Vision API Cloud VPN Compute Engine Container Builder Container Engine Container Registry Debugger Deployment Manager Error Reporting Genomics Google Service Control Jibe Cloud and Hub Stackdriver Logging Trace
Product APIs	Apps Activity API Calendar API Contacts API Drive REST API Gmail REST API Sheets API Sites API Tasks API	
Admin SDK APIs	Admin Settings API Calendar Resource API	

Domain Shared Contacts API
Directory API
Email Audit API
Email Settings API
Enterprise Licence Manager API
Groups Migration API
Groups Settings API
Reports API
Reseller API
SAML-based SSO API

Table 5 - ISO 27017:2015 Certification

4.4 ISO 27018:2014 Certification

ISO 27018 establishes controls that examine our privacy practices and contractual commitments around the use of customer data and provide transparency on the processing of that data. It confirms that:

- Google does not use customer data for advertising
- The data that our customers entrust with us remains the customer's
- Google provides our customers with tools to delete and export customer data
- Google scrutinizes third party requests for customer data and adheres to its contractual commitments regarding customer notification of such third-party requests
- Google is transparent about where our customer’s data is stored

More details of the certification can be found in the table below.

	G Suite	Cloud
Auditors	Ernst & Young CertifyPoint	Ernst & Young CertifyPoint
Services Covered	G Suite	Google Cloud Platform

	G Suite (Google Apps Unlimited)	
	G Suite for Education	
Products	Admin Console	App Engine
	App Maker	App Engine Flexible Environment
	Apps Script	BigQuery
	Calendar	Cloud Bigtable
	Chrome Device Management	Cloud Billing API
	Chrome Sync	Cloud CDN (Content Delivery Network)
	Classic Sites	Cloud Console
	Classroom (only G Suite for Education)	Cloud Data Loss Prevention API
	Cloud Identity	Cloud Dataflow
	Cloud Search	Cloud Datalab
	Contacts	Cloud Dataproc
	Docs	Cloud Datastore
	Drive	Cloud DNS (Domain Name System)
	Forms	Cloud Endpoints
	Gmail	Cloud Functions
	Google+	Cloud IAM (Identity & Access Management)
	Google Now	Cloud Jobs API
	Groups	Cloud Key Management Service
	Hangouts	Cloud Launcher
	Hangouts Chat	Cloud Load Balancing

Hangouts Meet

Inbox by Gmail

Jamboard

Keep

Sheets

Sites

Slides

Talk

Tasks

Vault

Cloud Machine Learning Engine

Cloud Mobile App

Cloud Natural Language API

Cloud Pub/Sub

Cloud Resource Manager

Cloud Router

Cloud SDK

Cloud Security Scanner

Cloud Shell

Cloud Source Repositories

Cloud Speech API

Cloud SQL

Cloud Storage

Cloud Translation API

Cloud Virtual Network

Cloud Vision API

Cloud VPN

Compute Engine

Container Builder

Container Engine

Container Registry

Debugger

Deployment Manager

Error Reporting

Genomics

		Google Service Control Stackdriver Logging Trace
Product APIs	Apps Activity API Calendar API Contacts API Drive REST API Gmail REST API Sheets API Sites API Tasks API	
Admin SDK APIs	Admin Settings API Calendar Resource API Domain Shared Contacts API Directory API Email Audit API Email Settings API Enterprise Licence Manager API Groups Migration API Groups Settings API Reports API Reseller API SAML-based SSO API	

Table 5 - ISO 27018:2014 Certification

Additional information can be found in the SOC 2 report. Contact your Google account representative for more. For the latest information on compliance, please visit the G Suite and GCP compliance sites.

5. Operational Security

5.1 Configuration and Change Management

Security Principle (link)	Confirmation
The status, location and configuration of service components (including hardware and software components) are tracked throughout their lifetime within the service.	G Suite and GCP meet this objective.
Changes to the service are assessed for potential security impact. Changes are managed and tracked through to completion.	G Suite and GCP meet this objective.

Google meticulously tracks the location and status of all equipment within our data centers, from acquisition to installation to retirement to destruction. This tracking is achieved using bar codes and asset tags. Metal detectors and video surveillance are used to help ensure no unauthorised equipment leaves the data center floor. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. When a hard drive is retired, authorized individuals verify that the disk is erased by writing 0's to the drive and performing a verification to help ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks begins with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

Google's configuration and change management processes have been reviewed as part of the ISO 27001 & ISO 27017 certification.

5.2 Vulnerability Management

Security Principle (link)	Confirmation
Potential new threats, vulnerabilities or exploitation techniques which could affect the service are assessed and corrective action is taken.	G Suite and GCP meet this objective.
Relevant sources of information relating to threats and/or vulnerability and exploitation techniques, relevant to the service are monitored by the service provider.	G Suite and GCP meet this objective.
The severity of threats and vulnerabilities relevant to the service are considered within the context of the service and this information is used to prioritise implementation of mitigations.	G Suite and GCP meet this objective.
Known vulnerabilities within the service are tracked until suitable mitigations have been deployed through a suitable change management process.	G Suite and GCP meet this objective.
Service provider timescales for implementing mitigations to vulnerabilities found to be present within the service are made available to consumers.	G Suite and GCP meet this objective.

Google uses a vulnerability management process that continuously scans for security threats. This management process employs a combination of commercially available and purpose-built in house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits.

Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team at Google is responsible for tracking and following up any detected vulnerabilities. The team tracks and actions upon these issues until they can verify that the vulnerabilities have been remediated.

In addition, Google maintains relationships with members of the security research community to track reported issues in Google services and open source tools.

More information about reporting security issues can be found in Google's Application Security Policy and Google Cloud Platform's Security Policy.

5.3 Protective Monitoring

Security Principle (link)	Confirmation
Events generated in service components required to support effective identification of suspicious activity are collected and fed into an analysis system.	G Suite and GCP meet this objective.
Effective analysis systems are in place to identify and prioritise indications of potential malicious activity.	G Suite and GCP meet this objective.

Google maintains a security monitoring program that focuses on the detection of threats using a combination of information gathered from internal network traffic analysis, employee actions on automated system escalations, and external (to Google) knowledge of vulnerabilities. Each of these components is described in the paragraphs below.

5.3.1 Network Traffic Analysis

Our internal network traffic is continuously inspected for suspicious behaviour. These inspections are performed using a combination of open source and commercial traffic capture tools. In addition to these tools, we have built a proprietary correlation system that supports the inspections and their subsequent analysis.

5.3.2 Automated System Escalations

Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff. These escalations are manually reviewed, investigated and resolved by our security staff

5.3.3 External Vulnerabilities

Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure. They actively review inbound security reports and monitor public mailing lists, blog posts, and wikis.

5.4 Incident Management

Security Principle (link)	Confirmation
Incident management processes are in place for the service and are enacted in response to security incidents. Pre-defined processes are in place for responding to common types of incident and attack.	G Suite and GCP meet this objective.
A defined process and contact route exists for the reporting of security incidents by consumers and external entities.	G Suite and GCP meet this objective.
A definition of a security incident in the service is published to consumers, along with the triggers and timescales for sharing such incidents with service customers.	G Suite and GCP meet this objective.
The content and format of security incident notifications for sharing information with consumers is published.	G Suite and GCP meet this objective.
The maximum timescales by which an incident will be investigated is published to consumers.	G Suite and GCP meet this objective.

Google has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of our systems or data. If an incident occurs, the security team logs and prioritizes the incident according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation.

Google's security incident management program is structured around the NIST guidelines on handling incidents, namely NIST SP 800–61. Key staff are trained in forensics and evidence handling in preparation for an event, including the use of third party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24x7 to all employees. If an incident

involves customer data, Google will inform the customer and assist with investigative efforts via our support team.

Google Security engineers conduct post-mortem investigations when necessary to determine the root cause for single events, trends spanning multiple events over time, and to develop new strategies to help prevent recurrence of similar incidents.

Incident management processes have been reviewed in the ISO 27001 & ISO 27017 certifications.

6. Personnel Security

Security Principle (link)	Confirmation
Service provider staff that have access to the service (physically or logically) or any potential ability to access consumer's data or affect the service, are subjected to adequate personnel security screening for their role. At a minimum, these checks include: identity, unspent criminal convictions, and right to work checks.	G Suite and GCP meet this objective.

6.1 Overview

Google has created a vibrant and inclusive security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, and as part of ongoing training, in addition to company-wide events to raise awareness.

6.2 Employee Background Checks

Before they join our staff, Google will verify a new hire's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, Google may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position.

6.3 Security Training for All Employees

All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

6.4 Internal Security and Privacy Events

Security and privacy is an ever evolving area and Google recognizes that dedicated employee engagement is a key means of raising awareness. We host regular internal conferences to raise awareness and drive innovation in security and data privacy. For example, we hold an annual “Privacy Week,” during which we host events across our global offices to raise awareness of privacy in area, from software development to data handling to policy enforcement, and living our privacy principles. In addition, we also host regular “Tech Talks” focusing on subjects that often include security and privacy. These conferences and events are open to all employees.

6.5 Our Information Security Team

At the center of the Google security model is our Information Security team consisting of more than 750 top experts in information, application, and network security. This team is tasked with maintaining the company’s defence systems, developing security review processes, building security infrastructure and implementing Google’s security policies.

Within Google, members of the Information Security team review security plans for all networks, systems and services. They provide project-specific consulting services to Google’s product and engineering teams. They monitor for suspicious activity on Google’s networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. Google has built a full-time team, known as Project Zero. The goal of this team is to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.

The Security Team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions.Their notable achievements include the discovery of the POODLE SSL 3.0 exploit and cipher suite weaknesses. The security team also publishes security research papers, which we make

available to the public. Lastly, the team organizes and participates in open-source projects and academic conferences.

6.6 Our Dedicated Privacy Team

The Google Privacy team operates independently from the product development and security organizations, but participates in every Google product launch. The team reviews design documentation and code audits to help ensure that privacy requirements are followed. The Privacy team has built a set of automated monitoring tools to help ensure that products with customer data operate as designed and in accordance with our privacy policy. They help release products that reflect strong our privacy standards: transparent collection of user data and providing users and administrators with meaningful privacy configuration options, while continuing to be sound stewards of any information stored on our platform. After products launch, the privacy team oversees automated processes that audit data traffic to verify appropriate data usage. In addition, the privacy team conducts research providing thought leadership on privacy best practices for our emerging technologies.

6.7 Our Internal Audit and Compliance Specialists

Google has a dedicated internal audit team that reviews compliance with security legislation and regulations globally. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team also facilitates and supports independent audits and assessments by third parties.

6.8 Our Collaboration With the Security Research Community

Google has long enjoyed a close relationship with the security research community, and we greatly value their help identifying any vulnerabilities in our products. Our Vulnerability Reward Program encourages researchers to report design and implementation issues that may put customer data at risk, offering rewards in the tens of thousands of dollars. For example, in Chrome, we warn users against malware and phishing, and offer rewards for finding security bugs. As a result of our collaboration with the research community, we have resolved more than 700 Chrome security bugs and have awarded more than $1.25 million. In total, more than $2 million has been awarded across all of Google's vulnerability rewards programs. We publicly thank these individuals and list them as contributors to our products and services.

Additional information can be found in the SOC 2 report. Contact your Google account representative for more.

7. Secure Development

Security Principle (link)	Confirmation
New and evolving threats are regularly reviewed. Development tasks are initiated to improve and reinforce the security of the service in line with changing threats	G Suite and GCP meet this objective.
Software development is carried out in line with industry best practice regarding secure design, coding, testing, and deployment.	G Suite and GCP meet this objective.
Software configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.	G Suite and GCP meet this objective.

7.1 Overview

It is Google's policy to consider the security properties and implications of applications, systems, and services used or provided by Google throughout the entire project lifecycle. Google's "Applications, Systems, and Services Security Policy" calls for teams and individuals to implement appropriate security measures in applications, systems, and services being developed, commensurate with identified security risks and concerns. The policy states that Google maintains a security team chartered with providing security-related guidance and risk-assessment.

Google employs a variety of measures to help ensure that the software products and services Google offers to its users meet high standards of software security. This section outlines Google's current approach to software security; it may adapt and evolve in the future.

7.2 Security Consulting and Review

With regards to the design, development, deployment and operation of applications and services, the Google Security Team provides the following primary categories of consulting services to Google's Product and Engineering Teams:

- **Security Design Reviews**: design-level evaluations of a project's security risks and corresponding mitigating controls, as well as their appropriateness and efficacy.
- **Implementation Security Reviews**: implementation-level evaluation of code artifacts to assess their robustness against relevant security threats.
- **Security Consulting**: ongoing consultation on security risks associated with a given project and possible solutions to security concerns, often in the form of an exploration of the design space early in project life cycles.

Google recognizes that many classes of security concerns arise at the product design level and therefore must be taken into consideration and addressed in the design phase of a product or service. Ensuring that such considerations are taken into account is the primary purpose of the Security Design Review.

As such, the security design review has the following objectives:

- provide a high-level evaluation of the security risks associated with the project, based on an exploration of relevant threats.
- equip the project's decision makers with the information necessary to make informed risk management decisions and integrate the consideration of security into project objectives.
- provide guidance on the choice and correct implementation of planned security controls, e.g., authentication protocols or encryption.
- help ensure that the development team is adequately educated with regard to relevant classes of vulnerabilities, attack patterns, and appropriate mitigation strategies.

In cases where projects involve innovative features or technologies, it is the Security team's responsibility to research and explore security threats, potential attack patterns, and technology-specific vulnerability classes related to such features and technologies.

Where appropriate, Google contracts with third party security consulting firms to complement the Google Security Team's skill set and to obtain independent third party review to validate in-house security reviews.

7.3 Security and Google's Software Lifecycle

Security is at the core of our design and development process. Google's Engineering organization does not require product development teams to follow a specific software development process; rather, teams choose and implement processes that fit needs of the project. As such, a variety of software development processes are in use at Google, from Agile Software Development methodologies to more traditional, phased processes.

Google's security reviews are adapted to work within the teams chosen development process. That this can be done successfully hinges on Google's quality-driven engineering culture and the requirements listed below as defined by Engineering management:

- peer-reviewed design documentation
- adherence to coding style guidelines
- peer code review
- multi-layered security testing

These mandates embody Google's software engineering culture, where key objectives include software quality, robustness, and maintainability. While the primary goal of these mandates is to foster the creation of software artifacts that excel in all aspects of software quality, they also represent significant and scalable drivers toward reducing the incidence of security flaws and defects in software design. Some examples:

- the existence of adequately detailed design documentation is a prerequisite of the security design review process, since in early project stages it is generally the only available artifact on which to base security evaluations.
- many, if not most, classes of implementation-level security vulnerabilities are fundamentally no different from low-risk, common functional defects caused by fairly straightforward oversights on the part of the developer.
- given developers and code reviewers who are educated with respect to applicable vulnerability patterns and their avoidance, a peer review-based development culture that emphasizes the creation of high-quality code is a very significant and scalable driver towards a secure code base.
- a peer review-based development culture that emphasises the creation of high quality code. Peer reviewers should be knowledgeable of security vulnerability patterns and their avoidance.

The Security team's software engineers collaborate with other engineers across Google on the development and vetting of reusable components designed and implemented to help software projects avoid certain classes of vulnerabilities. Examples of this include, database access layers designed to be inherently robust against query-language injection vulnerabilities, or HTML templating frameworks with built-in defenses against cross-site-scripting vulnerabilities (such as the Auto Escape mechanism in the open-sourced Google CTemplate library).

7.4 Security Education

Recognizing the importance of an engineering work force that is educated with respect to secure coding practices, the Google Security Team maintains an engineering outreach and education program that currently includes:

- Security training for new engineers.
- The creation and maintenance of extensive documentation on secure design and coding practices.
- Targeted, context-sensitive references to documentation and training material. For example, automated vulnerability testing tools provide engineers with references to training and background documentation related to specific bugs or classes of bugs flagged by the tool.
- Technical presentations on security-related topics.
- A security newsletter with engineering team-wide distribution that is intended to keep Google's engineering workforce abreast of new threats, attack patterns, mitigation techniques, security-related libraries and infrastructure, best practices and guidelines, etc.
- A recurring Google-wide conference called the Security Summit that brings together engineers from various teams at Google who work in security-related fields, and that offers in-depth technical presentations on security topics to Google Engineering at large.

7.5 Implementation-Level Security Testing and Review

Google employs a number of approaches to further reduce the incidence of implementation-level security vulnerabilities in its products and services:

- **Implementation-level security reviews**: conducted by members of the Google Security Team, typically in later stages of product development, implementation-level security reviews aim to validate that a software artifact has been developed to be robust against relevant security threats. Such reviews typically consist of a re-evaluation of threats and countermeasures identified during the security design review, targeted security reviews of security-critical code, selective code reviews to assess code quality from a security perspective, and targeted security testing.
- **Automated testing**: for flaws in certain relevant vulnerability classes. We use both in-house developed tools and some commercially available tools for this testing.
- **Security testing**: performed by Software Quality Engineers in the context of the project's overall software quality assessment and testing efforts.

8. Supply Chain Security

Security Principle (link)	Confirmation
The service provider informs consumers of how	G Suite and GCP meet this

much of their information is shared with, or accessible by, third party suppliers and their supply chains.	objective.
The service provider's procurement processes ensure that security requirements on third party suppliers and delivery partners are explicitly documented. These security requirements should include relevant requirements from the Cloud Security Principles.	G Suite and GCP meet this objective.
The risks to the service from third party suppliers and delivery partners are regularly assessed by the service provider and appropriate security controls implemented. The service provider monitors the conformance of their suppliers through security requirements and initiates remedial action where necessary.	G Suite and GCP meet this objective.
The service provider's procurement processes ensure that all assets relating to the service are returned, removed (or appropriately destroyed) and accesses to the service terminated.	G Suite and GCP meet this objective. The processes described here are certified in our ISO 27001, 27017 and SOC 2 documents.
The service provider has the necessary information and processes to verify that the hardware and software used in the service is genuine and has not been obviously tampered with.	G Suite and GCP meet this objective. The processes described here are certified in our ISO 27001, 27017 and SOC 2 documents.

8.1 Overview

Google's data centers house energy-efficient custom, purpose-built servers and network equipment that we design and manufacture ourselves. Unlike much commercially available hardware, Google servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, which can introduce vulnerabilities. Our production servers run a custom-designed operating system (OS) based on a stripped-down and hardened version of Linux. Google's servers and their OS are designed for the sole purpose of providing Google services. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on customer

demand. This homogenous environment is maintained by proprietary software that continuously monitors systems for binary modifications. If a modification is found that differs from the standard Google image, the system is automatically returned to its official state. These automated self-healing mechanisms are designed to enable Google to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential compromise on the network.

8.2 Google Group Subprocessors

Google Group entities engage personnel to provide service support and IT-facility management in connection with the services we provide. This support and management includes engineering activities related to managing the availability, latency, scalability and efficiency of the services we provide; product management; and customer outreach and support.

For more information on subprocessors, please see here for G Suite and here for GCP.

9. Secure Consumer Management

Security Principle (link)	Confirmation
Only authorized individuals from the customer organization are able to authenticate to and access manage interface for the service.	G Suite and GCP meet this objective.

Authentication of customers to management interfaces and within support channels varies by product. The sections below describe this authentication process for G Suite and GCP respectively.

G Suite

The G Suite Administration Console is your single place to manage all Google services: from settings for each individual service to user management. Within customer organizations, administrative roles and privileges for Google Suite are configured and controlled by the customer. This means that individual team members can manage certain services or perform specific administrative functions without gaining access to all settings and data. Integrated audit logs offer a detailed history of administrative actions, helping customers monitor internal access to data and adherence to their own policies.

To safeguard the security of your Google Suite account and help ensure that changes to your account are only made by authorized administrators from your organization, your Google Admin console contains a unique identifier for your account, known as a PIN. Your PIN may vary, depending on the product. For example, your PIN for Google Suite will be different than your PIN for Chrome Management.

More information on securely accessing the Administration Panel can be found in our Help Center.

Google Cloud Platform

GCP offers Cloud Identity and Access Management (IAM) which allows you to create and manage permissions for GCP resources. It unifies access control for Cloud Platform services into a single system and presents a consistent set of operations. Cloud IAM lets you adopt the security principle of least privilege, so you grant only the necessary access to your resources and prevent unwanted access to other resources. IAM allows you to meet compliance clauses around the separation of duty.

All Cloud Platform services use Cloud IAM to make sure that only authorized identities can access them. In addition, some services provide IAM roles specific to their services, or support granting access at the resource level.

To safeguard the security of your Google account and help ensure that changes to your account are only made by authorized administrators from your organization, the Google Developers Console contains a unique identifier for your account, known as a PIN. Calls to the support line require you to know your PIN, and PIN codes are regularly rotated.

Cloud IAM is subject to audit at least annually under: ISO 27001:2013, ISO 27018:2014, ISO 27017:2015 and SOC2. These certifications are recognised by ENISA under the Cloud Certification Schemes. The controls in relation to secure consumer management are validated independently at least annually under the certification programs.

More information on securely accessing Google Developers Console can be found in our Help Center.

The Google IAM API manages identity and access control for GCP resource, including the creation of service accounts which can be used to authenticate to Google and make API calls. This functionality gives better control and simplifies access management when managing services and resources across multiple Google accounts. For more information on the IAM API, see Google Identity and Access Management API.

10. Identity and Authentication

Security Principle (link)	Confirmation
Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorized individuals.	Both G Suite and GCP meet this requirement.

10.1 Overview

In this section, we outline the common and product specific identity and authentication technologies that support G Suite and GCP. First, the common technologies.

10.2 2-Step Verification

Google accounts (GCP and G Suite) support 2-Step Verification which adds an extra layer of security to your account by requiring users to enter a verification code in addition to their username and password, when signing into their account.

2-Step Verification helps protect a user's account from unauthorized access should someone manage to obtain their password. Even if a password is cracked, guessed, or otherwise stolen, an attacker can't sign in without access to the user's verification codes, which only the user can obtain via their own mobile phone. Learn more about 2-Step Verification.

The sections that follow outline identity and authentication technologies for G Suite and GCP respectively.

10.3 G Suite

10.3.1 SAML 2.0 Integration

G Suite offers customers a single sign-on (SSO) service that lets users access multiple services using the same sign-in page and authentication credentials. SSO is based on SAML 2.0, an XML standard that allows secure web domains to exchange user authentication and authorization data. For additional security, SSO accepts public keys and certificates generated with either the RSA or DSA algorithm. Customer organizations can use the SSO service to

integrate single sign-on for G Suite into their LDAP (Lightweight Directory Access Protocol) or other SSO system.

10.3.2 OAUTH 2.0 and OpenID Connect

G Suite supports OAuth 2.0 and OpenID Connect, an open protocol for authentication and authorization. This allows customers to configure one single sign-on service (SSO) for multiple cloud solutions. Users can log on to third-party applications through G Suite—and vice versa—without re-entering their credentials or sharing sensitive password information.

10.3.3 Agency Administrator Roles

You can share the responsibility of managing your Google enterprise account by assigning administrator roles to other users. Assigning a role grants the user access to your Google Admin console. You can make a user a super administrator who can perform all tasks in the Admin console or you can assign a role that limits which tasks the administrator can perform, for example, by allowing them only to create groups, manage service settings, or reset a user's password.

To get started with administrator roles:

- Review pre-built roles: We've created administrator roles for performing common business functions that you may be able to use out of the box—one role for managing users, another for groups, another for services, and so on.
- Create custom administrator roles: If the pre-built roles don't meet your needs, create your own custom roles. For each custom role, choose from the same set of privileges used in the pre-built roles, grouping them however you want.
- Assign roles to users: Assign administrator roles to users that let them perform the tasks you want them to manage. For roles that permit managing users, optionally assign the organizational unit you want them to manage.

10.3.4 User Management

With Google Cloud Directory Sync, you can automatically provision users, groups, and non-employee contacts based on the user data in your LDAP server, such as Microsoft Active Directory or Lotus Domino. Google Cloud Directory Sync connects to your G Suite directory and adds/deletes user accounts to match your existing organizational schema.

The Google Cloud Directory Sync configuration wizard guides you through customizing your synchronization and mapping of your LDAP user list to your G Suite users, nicknames, shared contacts, and groups. You can also synchronize rich user profile data like home/work/mobile

phone numbers, addresses, and job titles. To manage your synchronization, you can perform test synchronizations, and configure change limits, notifications, and scheduled synchronizations.

More information on Google Cloud Directory Sync can be found here.

10.4 Google Cloud Platform

Google's infrastructure does not assume any trust between services running on the infrastructure. In other words, the infrastructure is fundamentally designed to be multi-tenant. The following sections provide more detail.

10.4.1 Service Identity, Integrity, and Isolation

Google uses cryptographic authentication and authorization at the application layer for inter-service communication. This provides strong access control at an abstraction level and granularity that administrators and services can naturally understand.

We do not rely on internal network segmentation or firewalling as our primary security mechanisms, though we do use ingress and egress filtering in our network to prevent IP spoofing. This approach help us to maximize our network's performance availability.

Each service that runs on the infrastructure has an associated service account identity. A service is provided with cryptographic credentials that it can use to prove its identity when making or receiving remote procedure calls (RPC's) to other services. These identities are used by clients to help ensure that they are talking to the correct intended servicer and by servers to limit access to methods and data to particular clients.

Google's source code is stored in a central repository where both current and past versions of the service are auditable. The infrastructure can additionally be configured to require that a service's binaries be built from specific reviewed, checked in, and tested source code. Such code reviews require inspection and approval from at least one engineer other than the author. In addition, the system enforces that code modifications to any system must be approved by the owners of that system. These hard requirements limit the ability of an insider or adversary to make malicious modifications to source code and also provide a forensic trail from a service back to its source.

We have a variety of isolation and sandboxing techniques that protect a service from other services running on the same machine. These techniques include normal Linux user separation, language and kernel-based sandboxes, and hardware virtualization. In general, we use more layers of isolation for riskier workloads; for example, when running complex file format converters on user-supplied data or when running user supplied code for products like Google

App Engine or Google Compute Engine. As an extra precaution, we run certain sensitive services such as the cluster orchestration service exclusively on dedicated machines.

10.4.2 Inter-Service Access Management

The owner of a service can use access management features provided by the infrastructure to specify exactly which other services can communicate with it. For example, a service may want to offer some API's to a specific whitelist of other services. The service can be configured with the whitelist of the allowed service account identities and this access restriction is then automatically enforced by the infrastructure.

Google engineers accessing services are also issued individual identities so that services can be similarly configured to allow or deny their access. All of these identity types (machine, service, and employee) are in a global namespace that the infrastructure maintains. Customer identities are maintained separately, see section 10.4.3.

The infrastructure provides a rich identity management workflow system for these internal identities including approval chains, logging and notification. For example, these identities can be assigned to access control groups via a system that allows two party control. In this case, one engineer can propose a change to a group that another engineer (who is also an administrator of the group) must approve. This system allows secure access management processes to scale to the thousands of services running on the infrastructure.

10.4.3 Access Management of Customer Data

A typical Google service is written to do something for a customer. For example, a customer may store their email on Gmail. The customer's interaction with an application like Gmail spans other services within the infrastructure. So for example, the Gmail service may call an API provided by the Contacts service to access the customer's address book.

The Contacts service can be configured such that the only RPC requests that are allowed are from the Gmail service. This, however, is still a broad set of permissions. Within the scope of this permission the Gmail service would be able to request the contacts of any user at any time. Since the Gmail service makes an RPC request to the Contacts service on behalf of a particular customer, the infrastructure provides the ability for the Gmail service to present a "customer permission ticket" as part of the RPC. This ticket proves that the Gmail service is currently servicing a request on behalf of that particular customer. This enables the Contacts service to implement a safeguard where it only returns data for the customer named in the ticket.

The infrastructure provides a central user identity service which issues these "customer permission tickets". A customer login is verified by the central identity service which then issues a user credential such as a cookie or OAuth token, to the customer's client device. Every subsequent request from the client device into Google needs to present this customer credential

When a service receives a customer credential, it passes the credential to the central identity service for verification. If the customer verifies correctly, the central identity service returns a short lived “customer permission ticket” that can be used for RPC’s related to the request. In our example, that service which gets the “customer permission ticket” would be the Gmail service, which would pass it to the Contacts service. From that point on, for any cascading calls, the “customer permission ticket” can be handed down by the calling service to the callee as part of the RPC call.

For more information, see the Google Infrastructure Security Design Overview.

11. External Interface Protection

Security Principle (link)	Confirmation
The service provider informs consumers which networks the service is accessible from and what interfaces are exposed to those networks	G Suite and GCP meet this objective.
The service provider has protections in place to prevent unauthorised access to the service via any exposed interfaces by consumers or outsiders.	G Suite and GCP meet this objective.
The service provider publishes guidance to consumers on how to safely connect to the service whilst minimising risk to the consumer’s systems.	G Suite and GCP meet this objective.

11.1 G Suite

Google APIs use the OAuth 2.0 protocol for authentication and authorization. Google supports common OAuth 2.0 scenarios such as those for web server, installed, and client-side applications. A full overview on OAuth 2.0 and details on the scenarios that Google supports, see Using OAuth 2.0 for Login.

11.2 Google Cloud Platform

Google Cloud APIs are a key part of GCP, allowing our customers to easily add capabilities like storage access and machine-learning-based image analysis to their Cloud Platform applications. The Cloud APIs can be accessed from server applications using our client libraries.

For more information on our Google Cloud APIs, see Cloud API Overview.

12. Secure Service Administration

Security Principle (link)	Confirmation
The methods used by the services provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.	G Suite and GCP meet this objective.

The security of GCP is closely tied to the security of Google's administration systems. The design, implementation and management of these systems should mitigate any risk of exploitation by an attacker. The sections below outline the steps Google takes to secure its administration systems.

12.1 User Access

Google has policies and procedures in place that ensure that Google employees and contractor user accounts are added, modified, or disabled in a timely fashion and are reviewed on a regular basis. In addition, password complexity settings for user authentication to GCP systems are managed in compliance with Google's Corporate Password Policy.

12.2 Account Provisioning

Responsibility for the provision of employee and contractor access lies with our People Operations team and individual service owners. An employee or contractor account is provisioned in a disabled stated. The account is enabled when the employee's record is activated in our internal People Operations system. First time passwords are set to a unique value and are required to be changed on first use.

Access to other resources including Services, Host, Network devices and groups is explicitly approved in our proprietary permission management system by the appropriate owner or manager. Requests for changes in access are also captured in this system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked.

12.3 Periodic Account Review

Accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically removed.

12.4 Access Removal

Access is automatically removed when an employee's record is terminated in our People Operations system. Our permission management system removes the user in question from all systems.

12.5 Password Policy

Access and administration of logical security for Google relies on user ID's, passwords and security keys to authenticate users to services, resources and devices as well as to authorize the appropriate level of access to the user. Access to our tools and systems is logged and regularly audited.

12.6 Certification

The secure service administration principle and related processes within GCP services are subject to audit at least annually under: ISO 27001:2013, AICPA SOC 1, SOC 2, SOC 3 and PCI-DSS certification programs. These certifications are recognised by ENISA under the Cloud Certification Schemes. The controls in relation to secure consumer management are validated independently at least annually under the certification programs.

13. Audit Information Provision to Consumers

Security Principle (link)	Confirmation
The service provider makes consumers aware of the audit information that will be provided to them, how and when it will be made available to them, the format of the data, and the retention period associated with it.	G Suite and GCP meet this objective.

13.1 G Suite

G Suite provides reports and API's to our customers that allow them to monitor the services we provide to them.

13.1.1 Reports and Monitoring

A customer can monitor how individual Google services are being used and managed across their organization in the Admin console's Reports section. Here the customer can find tools to analyze their team's use of collaboration, identify unwanted security patterns, diagnose configuration problems, and much more. Full details can be found in our Reports and Monitoring help center.

13.1.2 G Suite Admin SDK

The G Suite Admin SDK allows Administrators to programmatically manage users, groups, licenses, Administrative Settings, Email Settings, Group Settings, Calendar Resources, Group Migration, Domain Shared Contacts and Data transfers. The Admin SDK can also be used to create reports. Full details can be found in our G Suite Admin SDK help center.

13.2 Google Cloud Platform

13.2.1 Implementation Tools

Cloud Audit Logs help customers with audit and compliance needs by enabling them to track the actions of administrators in their Google Cloud Platform projects, helping determine who did what, where and when in the account. The product consists of two log streams: Admin Activity and Data Access.

- Admin Activity audit logs contain an entry for every administrative action or API call that modifies the configuration or metadata for the related application, service or resource.

- Data Access audit logs contain an entry for every one of the following events:
    - API calls that read the configuration or metadata of an application, service or resource
    - API calls that create, modify or read user-provided data managed by a service

For more information, please see the product documentation and this blog post.

13.2.2 Compliance Audit Information

GCP meets rigorous privacy and compliance standards that test for data privacy, safety, privacy, and security. Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third party audits on a regular basis to provide this assurance. This means than an independent auditor has examined the controls present in our data centers, infrastructure, and operations.

We have annual audits for the following standards:

- SSAE16 / ISA3042 Type II:
    - SOC 1
    - SOC 2
    - SOC 3 public audit report
- ISO (see section 4):
    - ISO 27001
    - ISO 27017
    - ISO 27018
- FedRamp ATO for Google App Engine
- PCI DSS v3.1

Our third party audit approach is designed to be comprehensive in order to provide assurances of Google's level of information security with regard to confidentiality, integrity, and availability. Customers may use these third party audits to assess how our products can meet their compliance and data-processing needs. Learn more about GCP Compliance and view the most recent Compliance updates.

CSA Star: Google Cloud has completed the Cloud Security Alliance (CSA) STAR Self-Assessment. For more information see Google Cloud and CSA Star.

14. Secure Use of the Service by the Consumer

Security Principle (link)	Confirmation

Consumers have certain responsibilities when using a Cloud service in order for this use to remain secure, and for their data to be adequately protected.	G Suite and GCP meet this requirement.

14.1 G Suite

In addition to the domain-wide security settings described in section 10, each service has a set of security-relevant settings. As an example, this section describes the security related settings for a core G Suite service, Google Drive.

14.1.1 Google Drive

While allowing users to share documents outside an organization may seem less secure, it actually provides a simple, auditable, and recoverable mechanism for users to collaborate outside the domain. When users don't have the ability to share outside their domain, the most common fallback is to send attachments via email. In this case, once the attachments leave the domain, there is no way to control, audit, or revoke access.

Google Drive apps and add-ons utilize OAuth to request access to data stored within G Suite. These "tokens" can be audited within the Admin console or via API. Additionally, several third-party vendors have developed tools to automatically revoke unapproved apps and add-ons by removing their access tokens. If Drive apps are disabled, access to the Drive APIs is also prevented, except for apps installed from the G Suite Marketplace.

14.1.2 Service Usage Logs

G Suite offers multiple avenues through which a customer can get information on service usage. A customer can monitor how individual Google services are being used and managed across their organization in the Admin console's Reports section. Here there are tools to analyze your team's use of collaboration, identify unwanted security patterns, diagnose configuration problems, and understand how users create and share content. Some examples of these tools are listed below.

- **Usage graphs**: see at-a-glance, the organization's usage of individual service, such as the total email activity over the past month, or the number of documents being created and shared. Additionally, a customer can view service usage of mobile and Chrome devices. Some sample usage graphs:
    - active mail, calendar, and documents users
    - mailbox disk space usage
    - collaboration and sharing trends

    - active mobile and Chrome devices
- **Audit logs**: track specific user activities such as service settings made by other administrators, document edits, or access of Marketplace apps. Some examples of the type of audit logs:
    - Admin Audit: you can track exactly how your administrators are managing your account's core Google services, using the Admin console audit log. Here, you can see a history of which tasks have been performed in your Google Admin console, and by whom.
    - Marketplace Audit: you can monitor which G Suite G Suite Marketplace applications are being used in your domain, using the Marketplace Login Activity log. Specifically, this log lists each successful login to any Marketplace application you've installed in your domain's Google account. Included in the entry is the user who logged in and the event's date.
    - Drive & Docs audit: allows administrators to see when users view or edit Docs. This feature is specific to Docs and does not log use of Slides, Sheets, or other files within Google Drive. All Docs are included in the log except those changed via API or that are available publicly, which do not require authorization. If Docs auditing is enabled for a domain, then any access to a Doc owned by that domain from inside or outside the domain will be logged. The Docs audit log is an optional tool that you must first enable. Logs are collected for the period the Docs audit log is enabled.
- **Email log search**: view email delivery logs to track missing messages or troubleshoot other mail flow issues.
- **Additional (user behavior) reports**: monitor other specific user behaviors, such as disk-space consumption or email client choices.

The Reports section of the Google Admin console contains a number of additional reports that track specific user behaviors in your organization, such as the email clients they're using or their disk-space usage. Download the report you want to run (in CSV format), then open it in a spreadsheet or text editor.

14.2 Google Cloud Platform

Google Cloud Platform benefits from the security of our underlying infrastructure. As an example, this section describes the Google Compute Engine service specific security we have built on top of our infrastructure.

Compute Engine enables customers to run their own virtual machines on Google’s infrastructure. The Compute Engine implementation consists of several logical components, most notably the management control plane and the virtual machines themselves. The management control plane exposes the internal API surface and orchestrates tasks like virtual

machine creation and migration. It runs as a variety of services on the infrastructure, thus it automatically gets foundational integrity features such as a secure boot chain. The individual services run under distinct internal service accounts so that every service can be granted only the permissions it requires when making remote procedure calls (RPCs) to the rest of the control plane. The code for all of these services is stored in a central Google source code repository, and there is an audit trail between this code and the binaries that are eventually deployed.

The Compute Engine control plane exposes its API via the Google Front End (GFE), and so it takes advantage of infrastructure security features like Denial of Service (DoS) protection and centrally managed SSL/TLS support. Customers can get similar protections for applications running on their Compute Engine VMs by choosing the optional Google Cloud Load Balancer service which is built on top of the GFE and can mitigate many types of DoS Attacks

End user authentication to the Compute Engine control plane API is done via Google's centralized identity service which provides security features such as hijacking detection. Authorization is done using the central Cloud IAM service.

The network traffic for the control plane, both from the GFEs to the first service behind it and between other control plane services is automatically authenticated by the infrastructure and encrypted whenever it travels from one data center to another. Additionally, the infrastructure has been configured to encrypt some of the control plane traffic within the data center as well.

Each virtual machine (VM) runs with an associated virtual machine manager (VMM) service instance. The infrastructure provides these services with two identities. One identity is used by the VMM service instance for its own calls and one identity is used for calls that the VMM makes on behalf of the customer's VM. This allows us to further segment the trust placed in calls coming from the VMM.

Compute engine persistent disks are encrypted at-rest using keys protected from the central infrastructure management system. This allows for automated rotation and central auditing of access to these keys.

Customers have the choice of whether to send traffic from their VMs to other VMs or the internet in the clear, or to implement any encryption they choose for this traffic. All control control plane WAN traffic within the infrastructure is encrypted.

The isolation provided to the VMs based on hardware virtualization using the open source KVM stack. We have further hardened our implementation of KVM by moving some of the control and hardware emulation stack into an unprivileged process outside the kernel. We have also extensively tested the core of KVM using techniques like fuzzing, static analysis, and manual code review.

Finally, our operational security controls are a key part of making sure that accesses to data follow our policies. As part of the Google Cloud Platform, Compute Engine's use of customer data follows the GCP use of customer data policy, namely that Google will not access ou use customer data, except as necessary to provide services to customers.

Additional information can be found in the SOC 2 report, under the "G. Recommended User Entity Considerations" section. Contact your Google account representative for more.

Appendix

eDiscovery

Google Vault is an add-on for G Suite* that lets you retain, archive, search, and export your organization's email for your eDiscovery and compliance needs. Vault is web-based, so there's no need to install or maintain any software.

Vault provides the following eDiscovery services:

- **Email and chat archiving**: Set retention rules to control how long email messages and on-the-record chats are retained before they are removed from user mailboxes and deleted from Google systems. Learn about retention.
- **Legal holds**: Place legal holds on users to preserve all their emails and on-the-record chats indefinitely in order to meet legal or other retention obligations You can place legal holds on all content in a user's account, or target specific content based on dates and terms. Learn about holds.
- **Search**: Search your domain's email, attachments, on-the-record chats and documents in Google Drive. Administrators can search by user account, date, or keyword. Vault supports Boolean, Gmail-specific, and wildcard operator searches. Learn about search.
- **Export**: Export specific email, chat and documents to standard formats for additional processing and review. Learn about exporting.
- **Audit reports**: Use Vault audit reports to learn about actions Vault users have taken during a specified period of time. Learn about audits.

**Vault is not available for all G Suite products. It is available for business and enterprise customers.*

Email Logs

Email log search gives G Suite administrators the ability to sift through the last month of delivery logs for their domains and evaluate message transit. This is useful for tracking down a sender or recipient's missing messages, such as those that have been quarantined as spam or otherwise routed incorrectly. Use this tool to determine the IP addresses sending and receiving mail or troubleshoot how policies affect mail flow. Only super administrators have access to email log search.

Customer Responsibility Controls

This section describes those additional policies, procedures and controls that Google recommends user entities consider to complement Google's policies, procedures and controls. The user entity's auditor should consider whether the controls below have been placed in operation at the user entity.

1. Classification of information

The customer is solely responsible for their Applications, Projects, and Data. The customer should classify their information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

2. Handling of assets

The customer is solely responsible for their Applications, Projects and Data. The customer should create groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this.

3. Identification of applicable legislation and contractual requirements

Customers should document how the organization's legal, regulatory and contract requirements map to the information supplied in Google's Cloud Platform Terms of Service including relevant amendments; information published by Google; and Google supplied audit reports.

4. Intellectual property rights

Customers should ensure that end-users are trained to use the Services consistent with the Acceptable Use Policies and Terms of Service.

5. Event logging

Customers should review and save, as necessary, audit reports available in their Services.

6. Protection of log information

Customers should protect audit logs stored offline, outside of the Services, against tampering and unauthorized access.

7. Administrator and operator logs

a. Customers should review and save, as necessary, audit reports available in the Services.

b. Customers should define and periodically review and update auditable events and review alerts generated by the system.

8. Monitoring of Cloud Services

a. Customers should review and save, as necessary, audit reports available in the Services.

b. Customers should define and periodically review and update auditable events and review alerts generated by the system.

9. Change management

a. Customers should periodically review the configuration of the Services to ensure it's consistent with organizational policies and procedures.

b. Customers should define and periodically review and update auditable events and review alerts generated by the system.

10. Separation of development, testing and operational environments

Customers should review feature and product releases and evaluate their impact consistent with the organization's needs.

11. Information security requirements analysis and specification

Customers should ensure the organization's information security requirements are considered in the deployment, configuration and modification of their instance of the Service.

12. System acceptance testing

Customers should review feature and product releases and evaluate their impact consistent with the organization's needs.

13. Protection of test data

The customer should configure testing environments in their instance of the Services, as applicable, and restrict access to data in these environments.

14. Responsibilities and procedures

a. Customers should establish responsibilities and procedures to respond to information security incidents pertaining to the use of the Services.

b. 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 the Services.

15. Reporting information security events

a. Customers should establish responsibilities and procedures to respond to information security incidents pertaining to the use of the Services.

b. 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 the Services.
c. Customers should assess audit events and take action consistent with its incident response procedures.

16. Assessment of and decision on information security events

Customers should establish responsibilities and procedures to respond to information security incidents pertaining to the use of the Services.

17. Response to information security incidents

a. Customers should establish responsibilities and procedures to respond to information security incidents pertaining to the use of the Services.
b. 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 the Services.
c. Google Cloud Platform provides tools, such as Google Cloud Logging and Google Cloud Monitoring, that make it easy to collect and analyze request logs and monitor the availability of customer infrastructure services (e.g. VM instances). These tools also make it easy for the customer to create custom dashboards and set alerts when issues occur.

18. Learning from information security incidents

a. Customers should establish responsibilities and procedures to respond to information security incidents pertaining to the use of the Services.
b. 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 the Services.
c. Google Cloud Platform provides tools, such as Google Cloud Logging and Google Cloud Monitoring, that make it easy to collect and analyze request logs and monitor the availability of customer infrastructure services (e.g., VM instances). These tools also make it easy for the customer to create custom dashboards and set alerts when issues occur.

19. Collection of evidence

a. Customers should establish responsibilities and procedures to respond to information security incidents pertaining to the use of the Services.

b. 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 the Services.

20. Access control policy

Customers should establish, document and review policies and procedures addressing the customer's administration of access to the Services.

21. Information access restriction

a. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
b. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

22. Secure log-on procedures

a. Customers should implement secure log-on procedures to access the Services consistent with the organization's access policies.
b. Customers should enforce the use of 2-Step Verification on Super Administrator accounts.
c. Google recommends that customers use of a form of multi-factor authentication for all user accounts.

23. Password management system

a. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
b. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

24. Use of privileged utility programs

a. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access

(authentication and authorization) on all components and services on Google Cloud Platform Projects.

b. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

25. User registration and de-registration

a. Customers should establish, document and review policies and procedures addressing the Customer's administration of access to the Services.

b. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.

c. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

26. User access provisioning

a. Customers should provision user access and sharing permissions within the Services consistent with organizational policies.

b. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.

c. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

27. Management of privileged access rights

a. Customers should provision user access and sharing permissions within the Services consistent with organizational policies.

b. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.

c. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

28. Management of secret authentication information of users

a. Customers should establish procedures to allocate the initial password to access the Services to end-users.
b. Customers should enforce the use of 2-Step Verification on Super Administrator accounts.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

29. Review of user access rights

a. Customers should review users' access rights periodically, consistent with organizational policies.
b. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
c. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

30. Removal or adjustment of access rights

a. Customers should review users' access rights periodically, consistent with organizational policies.
b. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
c. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

31. Use of secret authentication information

a. Customers should train users on the use and disclosure of passwords used to authenticate to the Services.
b. Customers should enforce the use of 2-Step Verification on Super Administrator accounts.
c. Google recommends that Customers use of a form of multi-factor authentication for all user accounts.
d. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
e. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

32. Information transfer policies and procedures

Customers should establish, document and review policies and procedures addressing transfer and sharing of information within the organization and with external parties.

33. Agreements on information transfer

Customers should establish, document and review policies and procedures addressing transfer and sharing of information within the organization and with external parties.

34. Electronic messaging

The customer should ensure that web browsers used by end-users to interact with the Services support strong transport security.

35. Securing application services on public networks

The customer should ensure that web browsers used by end-users to interact with the Services support strong transport security.

36. Protecting application services transactions

The customer should ensure that web browsers used by end-users to interact with the Services support strong transport security.

37. Administrator's operational security

a. It is the customer's responsibility to define procedures for administrative operations and monitoring of their Google Cloud projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform

resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings.

c. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
d. Google Cloud Platform provides tools, such as Google Cloud Logging and Google Cloud Monitoring, that make it easy to collect and analyze request logs and monitor the availability of customer infrastructure services (e.g., VM instances). These tools also make it easy for customers to create custom dashboards and set alerts when issues occur.

38. Documented operating procedures

a. Customers should define, document and make available to users operating procedures for the operation of their instance of the Services.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings.
c. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.

39. Installation of software on operational systems

a. It is the customer's responsibility to implement appropriate procedures to control the implementation and configuration of products and services within their Google Cloud Platform projects. Customers are also responsible to implement procedures for engineering secure systems and applications within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

40. Restrictions on software installation

a. It is the customer's responsibility to implement appropriate procedures to control the implementation and configuration of products and services within their Google Cloud Platform projects. Customers are also responsible to implement procedures for engineering secure systems and applications within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

41. Segregation of duties

Customers should provision user access and sharing permissions within the Services consistent with organizational policies.

42. Information security policy for supplier relationships

a. Customers should document how the organization's legal, regulatory and contract requirements map to the information supplied in Google's Terms of Service including relevant amendments; information published by Google; and Google supplied audit reports.
b. Customers should opt into the Data Processing and Security Terms offered through the Services' Admin Panel, as appropriate.

43. Addressing security within supplier agreements

a. Customers should document how the organization's legal, regulatory and contract requirements map to the information supplied in Google's Terms of Service including relevant amendments; information published by Google; and Google supplied audit reports.
b. Customers should opt into the Data Processing Amendment offered through the Services' Admin Panel, as appropriate.

44. Information security awareness, education and training

a. Customers should ensure that end-users are trained to use the Services consistent with the Acceptable Use Policies and Terms of Service.
b. Customers should ensure that end-users are trained on the organizational policies and procedures relevant to the Services.

45. Removal of Cloud Service customer assets

The customer should ensure that Customer Data is exported and deleted from the Services before or within a reasonable amount of time after termination.

46. Privacy and protection of personally identifiable information

Customers should opt into the Data Processing Amendment offered through the Services' Admin Panel, as appropriate.

47. Independent review of information security

Customers should periodically review the configuration of the Services to ensure it's consistent with organization policies and procedures.

48. Compliance with security policies and standards

Customers should periodically review the configuration of the Services to ensure it's consistent with organization policies and procedures.

49. Technical compliance review

Customers should periodically review the configuration of the Services to ensure it's consistent with organization policies and procedures.

50. Controls against malware

a. Customers should ensure that end-users are trained on the organizational policies and procedures relevant to the Services.
b. The customer should ensure that web browsers used by end-users to interact with the Services support strong transport security.

51. Policies for information security

Customers should review its information security policies and the security capabilities in the Services to determine their applicability to the Services and modify or add policies as appropriate.

52. Review of the policies for information security

a. Customers should review its information security policies and the security capabilities in the Services to determine their applicability to the Services and modify or add policies as appropriate.
b. Google recommends that customer consider Google's Security Best Practices when establishing their security procedures and configuring their domain.

53. Information security roles and responsibilities

Customers should assign responsibilities for the operation and monitoring of cloud services.

54. Mobile device policy

Customers should configure the Services' mobile device options consistent with organization policies and procedures.

55. Inventory of assets (GCP)

a. It is the customer's responsibility to implement appropriate procedures to track and manage all virtual instances and services used within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.

56. Ownership of assets (GCP)

a. It is the customer's responsibility to implement appropriate procedures to track and manage all virtual instances and services used within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.

57. Acceptable use of assets (GCP)

a. It is the customer's responsibility to implement appropriate procedures to track and manage all virtual instances and services used within their Google Cloud Platform projects.

b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.

58. Return of assets (GCP)

a. It is the customer's responsibility to implement appropriate procedures to track and manage all virtual instances and services used within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.

59. Secure development policy (GCP)

a. It is the customer's responsibility to implement appropriate procedures to control the implementation and configuration of products and services within their Google Cloud Platform projects. Customers are also responsible to implement procedures for engineering secure systems and applications within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

60. System change control procedures (GCP)

a. It is the customer's responsibility to implement appropriate procedures to control the implementation and configuration of products and services within their Google Cloud Platform projects. Customers are also responsible to implement procedures for engineering secure systems and applications within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

61. Policy on the use of cryptographic controls (GCP)

a. It is the customer's responsibility to restrict access to cryptographic key files to only those who need it. Customers should make sure to set appropriate permissions on these files and consider encrypting these files using additional tools.
b. Google Compute Engine encrypts all data at rest. Compute Engine handles and manages this encryption for customers without any additional actions on your part. However, if customers wanted to control and manage this encryption yourself, customers can provide your own encryption keys.

62. Regulation of cryptographic controls (GCP)

It is the customer's responsibility to ensure that any cryptographic controls they they implement and manage on Google Cloud Platform are used in compliance with all relevant agreements, legislation and regulations.

63. Reporting information security weaknesses (GCP)

Employees and contractors using the organization’s information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.

64. Key management (GCP)

a. It is the customer's responsibility to restrict access to cryptographic key files to only those who need it. Customers should make sure to set appropriate permissions on these files and consider encrypting these files using additional tools.
b. Google Compute Engine encrypts all data at rest. Compute Engine handles and manages this encryption for customers without any additional actions on your part. However, if customers wanted to control and manage this encryption yourself, customers can provide your own encryption keys.

65. Capacity management (GCP)

a. Customers are responsible for their capacity planning and ensuring that Google Cloud Platform services and resources they use are monitored and provisioned to meet their required level of system performance.
b. Google Cloud Platform provide multiple capabilities for customers to manage their capacity efficiently and effectively.
c. Managed instance groups offer autoscaling capabilities that allow you to automatically add or remove instances from a managed instance group based on increases or decreases in load. Autoscaling helps your applications gracefully handle increases in traffic and reduces cost when the need for resources is lower.
d. App Engine applications automatically scale based on incoming traffic. Load balancing, microservices, authorization, SQL and noSQL databases, memcache, traffic splitting, logging, search, versioning, roll out and roll backs, and security scanning are all supported natively and are highly customizable.

66. Access control to program source code (GCP)

a. The customer is solely responsible for their Applications, Projects and Customer Data which include the source code for their applications.
b. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
c. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

67. Virtual Machine Hardening (GCP)

Google Compute Engine and Google Container Engine are powered by virtual machines (VM). If you use these technologies in your projects, it is your responsibility to keep the VM operating system and applications up to date with the latest security patches. Google maintains security and patching of the virtual machine environment.

68. Access to networks and network services (GCP)

a. Customers should establish, document and review policies and procedures addressing the customer's administration of access to the Services.
b. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
c. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

69. Clock synchronisation (GCP)

a. Customers are responsible to ensure that clocks of their Compute Engine instances are synchronized to a single reference time source.
b. It is recommended that all Compute Engine virtual machine instances are configured to use the internal Google NTP services.

70. Consistency between virtual and physical networks (GCP)

a. It is the customer's responsibility to ensure that networking within the Google Cloud Platform is configured to protect information in their systems and applications and in accordance to their network security policy.
b. Google Cloud Platform provides a configurable and flexible networking system that enables you to permit connections between the outside world and their instances. Customers can manage the network within their project by configuring the network, firewall, and instance settings.

71. Network Controls (GCP)

a. It is the customer's responsibility to ensure that networking within the Google Cloud Platform is configured to protect information in their systems and applications and in accordance to their network security policy.
b. Google Cloud Platform provides a configurable and flexible networking system that enables you to permit connections between the outside world and their instances. Customers can manage the network within their project by configuring the network, firewall, and instance settings.

72. Security of network services (GCP)

a. It is the customer's responsibility to ensure that networking within the Google Cloud Platform is configured to protect information in their systems and applications and in accordance to their network security policy.

b. Google Cloud Platform provides a configurable and flexible networking system that enables you to permit connections between the outside world and their instances. Customers can manage the network within their project by configuring the network, firewall, and instance settings.

73. Segregation in networks (GCP)

a. It is the customer's responsibility to ensure that networking within the Google Cloud Platform is configured to protect information in their systems and applications and in accordance to their network security policy.
b. Google Cloud Platform provides a configurable and flexible networking system that enables you to permit connections between the outside world and their instances. Customers can manage the network within their project by configuring the network, firewall, and instance settings.

74. Technical review of applications after operating platform changes (GCP)

a. It is the customer's responsibility to implement appropriate procedures to control the implementation and configuration of products and services within their Google Cloud Platform projects. Customers are also responsible to implement procedures for engineering secure systems and applications within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

75. Restrictions on changes to software packages (GCP)

a. It is the customer's responsibility to implement appropriate procedures to control the implementation and configuration of products and services within their Google Cloud Platform projects. Customers are also responsible to implement procedures for

engineering secure systems and applications within their Google Cloud Platform projects.

b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

76. Secure system engineering principles (GCP)

a. It is the customer's responsibility to implement appropriate procedures to control the implementation and configuration of products and services within their Google Cloud Platform projects. Customers are also responsible to implement procedures for engineering secure systems and applications within their Google Cloud Platform projects.
b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.

77. Secure development environment (GCP)

a. It is the customer's responsibility to implement appropriate procedures to control the implementation and configuration of products and services within their Google Cloud

Platform projects. Customers are also responsible to implement procedures for engineering secure systems and applications within their Google Cloud Platform projects.

b. Google Cloud Platform provides container resources such as Organizations and Projects, that allow customers to group and hierarchically organize other Cloud Platform resources. This hierarchical organization lets customers easily manage common aspects of your resources such as access control and configuration settings. The Google Cloud Resource Manager API enables customers to programmatically manage these container resources.
c. Google Cloud Platform enables customers to adopt multiple approaches for authorization and authentication across the various components and services of the Platform. There are many factors for customers to consider when configuring access (authentication and authorization) on all components and services on Google Cloud Platform Projects.
d. It is the customer's responsibility to provide due care and consideration necessary to implement appropriate authentication and authorization mechanisms within their projects such that they protect their applications and assets from unauthorized access.