Google Cloud Whitepaper

October 2024

Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY 2023)

Google Cloud

This content was last updated in October 2024, and represents the current state as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Google Cloud

Introduction

National administrative organs, Incorporated Administrative Agencies, and Designated Corporations (hereinafter referred to as "Agencies") in Japan are required to implement appropriate security control measures for information systems by referring to and complying with the “Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies” (hereinafter referred to as "Common Standards") in the “Common Standards Group for Cybersecurity Measures for Government Agencies and Related Agencies” (final revision on July 4, 2023) (hereinafter referred to as "Common Standards Group") established by the National center of Incident readiness and Strategy for Cybersecurity (hereinafter referred to as "NISC").

In the FY2023 revision of the Common Standards, the level of security required for selected cloud services used by Agencies including Central Government Ministries and Agencies must be equal to or higher than the control standards required by the Information system Security Management and Assessment Program (ISMAP) as described in section "4.2 Use of Cloud Services " in the "Guidelines for Establishing Agencies' Standards for Information Security Measures", “Uniform Standards for Cybersecurity Measures for Government Agencies", "Guidelines for the Development of Countermeasure Standards for Government Agencies".

In addition, cloud services are required to be selected from the ISMAP Cloud Service List. After selection, when using cloud services, it is also important to utilize the functions provided by cloud services to build and operate information systems for Agencies on cloud services.

Google provides cloud services that comply with ISMAP control standards. Google is committed to helping Agencies that use our cloud services to comply with the Common Standards, by offering a secure infrastructure for building information systems, tools that support security, and education on how to utilize these tools. This document will explain how Agencies can use cloud services provided by Google to comply with the Common Standards.

This document is intended to be for informational purposes only. Nothing in this whitepaper is intended to provide you with, or should be used as, a substitute for legal advice.

Google Cloud

Common Standards

Structure of the Common Standards Group

NISC has formulated the “Common Standards Group for Cybersecurity Measures for Government Agencies and Related Agencies” (final revision on July 4, 2023) (hereinafter referred to as "Common Standards Group"), based on Article 26, Paragraph 1, Item 2 of the Basic Act on Cybersecurity (Act No. 104 of 2014).

The Common Standards Group is a unified framework for improving the information security level of Agencies by stipulating information security baselines as well as measures to ensure a higher level of information security.

As shown in Figure 1, the Common Standards Group consists of three documents: “Common Model of Cybersecurity Measures for Government Agencies and Related Agencies”, “Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY2023)", and “The Guidelines for Establishing Agencies’ Standards for Information Security Measures (FY2023)".

“Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY2023)" which is the subject of this document, are information security measures that are commonly required for all Agencies and stipulates matters that Agencies should comply with each item of the information security measures.

Figure 1: Positioning of the Common Standards

Google Cloud

Requirements from the Common Standards

The Common Standards consist of 8 parts, and the requirements for each part are shown in Table 1. Mainly in parts 4, 6, and 7 of the requirements of the Common Standards, Agencies, as users of cloud services, are required to confirm the security measures of the service infrastructure of cloud service providers. Specific security requirements corresponding to the standards can be confirmed through the links found in the column in Table 1 entitled "Items of the Common Standards."

Chapters	Items of the Common Standards	Requirements
1	General Provisions	Define the purpose of the Common Standards and the scope of application.
2	Basic Framework of Information Security Measures	Establish the structure of the organization and the information security measure promotion structure required by each organization.
3	Information Handling	Classify information from the viewpoint of confidentiality, integrity, and availability, and handle it according to the classification and place of processing.
4	Outsourcing	Establish outsourcing criteria and selection criteria of subcontractors, and ensure that information security measures are appropriately implemented, including at subcontractors. **Key points when selecting a cloud service** - In principle, you should select a cloud service from a cloud service list such as ISMAP. - When using cloud services, you should ensure that it meets the selection criteria and that information security measures are in place during procurement, operation, and termination. - If the cloud service outsources some of its services, you should also pay attention to whether the supplier is being properly managed.
5	Lifecycle of Information Systems	Implement necessary information security measures in a series of cycles from equipment procurement to development, construction, operation, maintenance, renewal, and disposal according to the Information System Lifecycle.
6	Information System Components	Implement information security measures for Terminals, Server Equipment, Communication Line Equipment, etc. **Key points when selecting a cloud service** - When using cloud services, it is expected that similar

Chapters	Items of the Common Standards	Requirements
		measures will be taken for virtual servers and virtual networks.
7	Security Requirements for Information Systems	Implement preventive security measures such as authentication/authorization and access control for information systems, and detective security measures such as system log retrieval and management. And also, take specific measures regarding vulnerability management and countermeasures against cyber-attacks. In addition, the 2023 revision also added measures for implementing and operating "Zero Trust Architecture.". **Key points when selecting a cloud service** - When using cloud services, it is necessary to check whether measures to prevent unauthorized access are properly stipulated and implemented on the service platform side.
8	Use of Information Systems	When using the system, users of government organizations should continuously take appropriate information security measures.

Table 1 : Requirements from the Common Standards

Relationship between the Common Standards and ISMAP

The scope of measures to be taken by cloud service customers/providers in accordance with the Common Standards are shown in Figure 2.

The measures required by the cloud service providers are defined in the ISMAP control standards. The cloud services that are determined to meet ISMAP control standards will be registered in the ISMAP Cloud Service List. By confirming that cloud services provided by Google are registered in the ISMAP Cloud Service List, Agencies can confirm that the level of security measures on the part of cloud service providers meets the government's security requirements.

On the other hand, in order for the information systems of Agencies to meet the Common Standards, as a cloud service customer and an entity that manages information systems, there are many items that should be implemented under the responsibility of Agencies, and simply checking the registered contents of the ISMAP Cloud Service List is not a sufficient measure. For example, Agencies must establish policies for handling information in applications developed on cloud services and access management processes that use the authentication and authorization functions of cloud services.

Agencies can take measures to meet the requirements of the Common Standards by utilizing various services of Google Cloud.

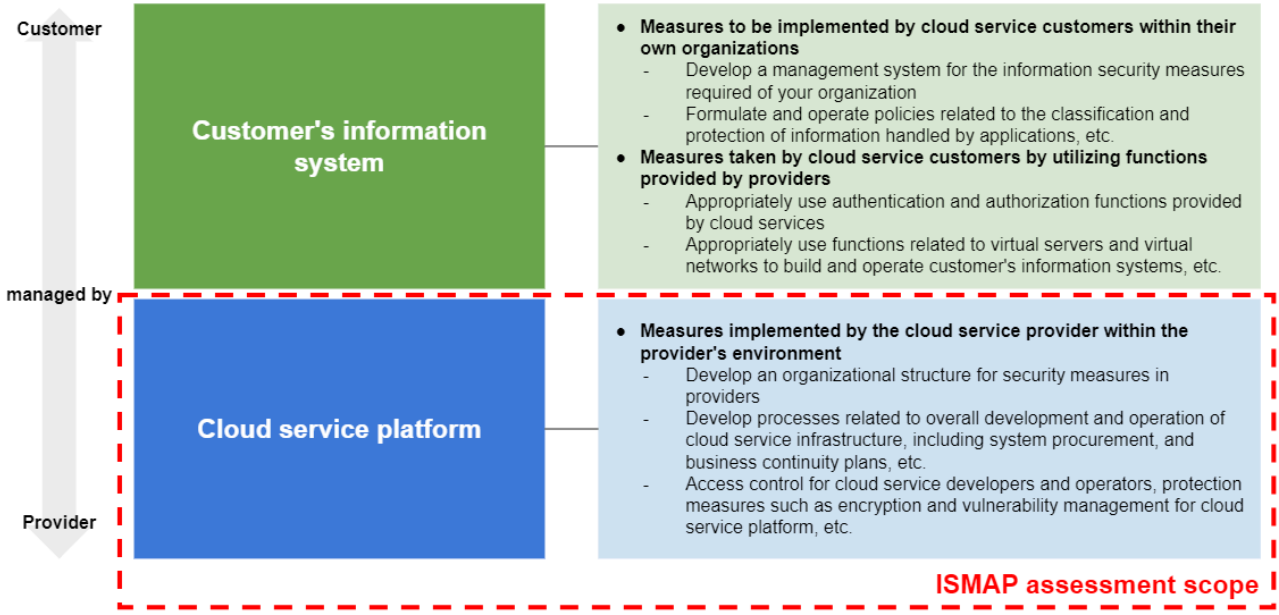


Figure 2: Scope of measures for cloud service customers/providers to comply with the Common Standards

Security Requirements and Measures

Shared Responsibility Model

Google is responsible for the security of the cloud infrastructure while our customers are responsible for the security in their cloud environment.
Google provides a shared responsibility model as a framework for these assumptions.

Google Cloud provides a wide range of services and features to help cloud service Customers fulfill their responsibilities under the shared responsibility model. In the following sections, we have organized the measures to meet the requirements of Common Standards into "Related Measures".

The following table shows the corresponding Related Measures that address the Requirements from each section of the Common Standards, with the exception of Part 1 (General Provisions) of the Common Standards. Details of each measure are described in the "Google Cloud Security & Services" section and can be found via the links in the table below.

Google Cloud

Basic Framework of Information Security Measures

Requirement	Related Measures
Have a mechanism for the detection and reporting of Information Security Incidents.	Logging Threat Detection Risk Detection
Provide training on the handling of information.	Training & Consultation
Make it possible to conduct audits to ensure the effectiveness of information security measures.	Logging Data Governance
Manage information related to the security requirements of information systems.	Security in our contracts Data Transformation

Information Handling

Requirement	Related Measures
Identify information held by the organization to implement safeguards for the handling of information.	Data Governance
Handle information appropriately according to information life cycle.	Access Controls Data Transformation Backup and Resilience Data Deletion
Control and limit the areas where information is handled.	Security in our infrastructure

Outsourcing

Requirement	Related Measures
Enable agencies to control access to information by outsourced personnel.	Identity Access Controls Data Governance
Verify the application status of various certification and accreditation systems as security requirements for cloud services.	Security and Compliance
Based on the utilization criteria for cloud services	Security in our contracts Security in our infrastructure Managing Third Party Suppliers

established by government agencies and other entities, verify whether the security measures of the cloud services meet the requirements.	
Develop and operate a secure system using cloud services.	Data Governance Data Transformation Data Deletion Secure CI/CD Pipeline Managed Services Partner Solutions
When configuring cloud services, refer to the recommended settings provided by the cloud service provider, industry standards, and best practices.	Risk Detection

Lifecycle of Information Systems

Requirement	Related Measures
Establish appropriate security requirements according to the functionality of the information systems used.	Data Governance Data Transformation Data Deletion Secure CI/CD Pipeline Managed Services Partner Solutions
Select equipments that can adequately implement information security measures.	Security in our infrastructure
Confirm that the business continuity plan and the information system operation continuity plan are consistent with the information security measures.	Backup and Resilience

Information Systems Components

Requirement	Related Measures
Use security technology to protect devices used by agencies from malware and unauthorized access.	Endpoint
Protect server equipment running information systems provided by agencies from security threats.	Managed Services Data Deletion Security in our infrastructure
Maintain availability, confidentiality, and integrity	Managed Services

for the various platforms running on the server.	
Control and monitor network access and protect against unauthorized access and attacks.	Access Controls Logging Security in our infrastructure

Security Requirements for Information Systems

Requirement	Related Measures
Ensure that only appropriate persons have access to information or information systems of agencies.	Identity Access Controls Data Governance
Capture and manage logs, and analyze and detect threats and attacks.	Logging Threat Detection
Encrypt data and resources to prevent information leakage and falsification.	Data Transformation
Continuously assess vulnerabilities in information systems and software.	Risk Detection
Prevent fraud and attacks through applications provided by government agencies.	Secure CI/CD Pipeline Risk Detection

Use of Information Systems

Requirement	Related Measures
Protect information systems from unauthorized changes and improper operation.	Managed Services Threat Detection Risk Detection Training & Consultation
Ensure that authentication and encryption policies are followed when staff use information systems.	Identity Data Transformation Training & Consultation

Google Cloud Security & Services

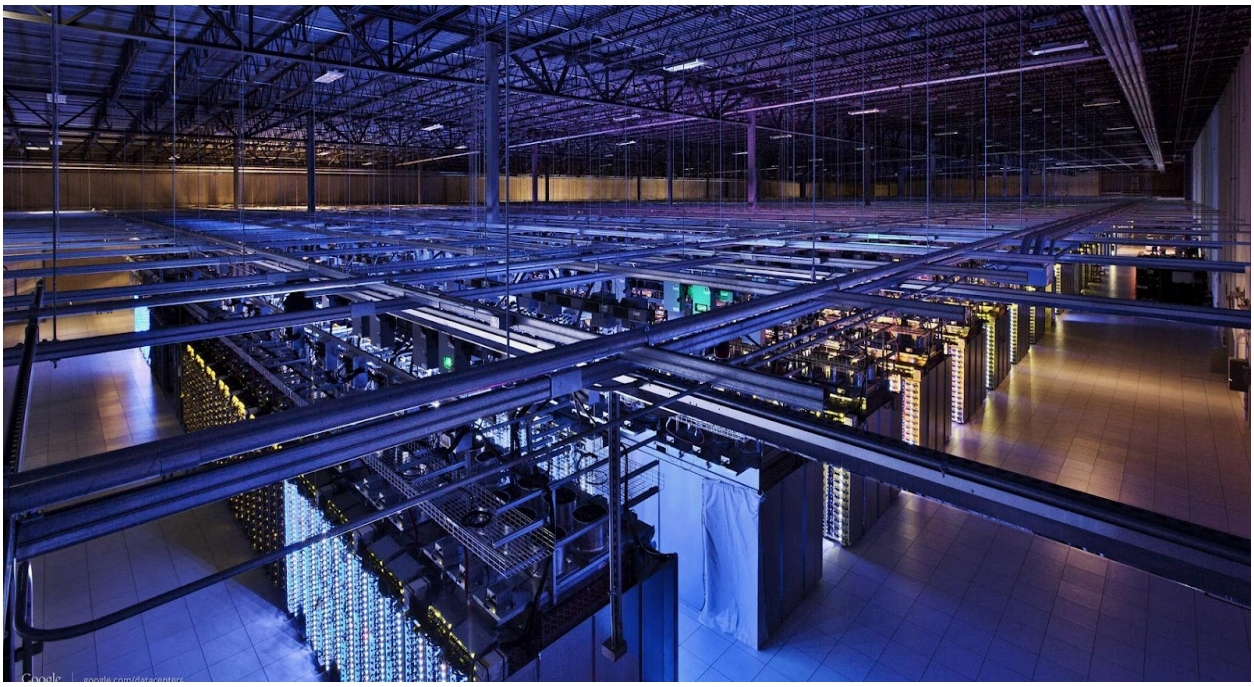
The following sections detail the services and technical measures introduced as "Related Measures" in the previous section.

Google Cloud

Security in our infrastructure

Google operates global infrastructure designed to provide state-of-the-art security through the information processing lifecycle. This infrastructure is built to provide secure deployment of services, secure storage of data with end-user privacy safeguards, secure communications between services, secure and private communication with customers over the Internet, and safe operation by administrators.

We designed the security of our infrastructure in layers that build upon one another, from the physical security of data centers, to the security protections of our hardware and software, to the processes we use to support operational security. A detailed discussion of our Infrastructure Security can be found in our Google Infrastructure Security Design Whitepaper.



The server hardware and network equipment that constitute the foundation of Google Cloud are also designed and procured to protect against intrusions and vulnerabilities.

Our data centers have purpose-built servers and network equipment, some of which we design ourselves. While our servers are customized to maximize performance, cooling, and power efficiency, they are also designed to help protect against physical intrusion attacks. Unlike most commercially available hardware, our servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, all of which can introduce vulnerabilities. We vet component vendors and choose components with care, working with vendors to audit and validate the security properties that are provided by the components. We design custom chips, such as Titan, that help us securely identify and authenticate legitimate Google devices at the hardware level, including the code that these devices use to boot up.

Google Cloud

Security in our contracts

Our Google Cloud data processing terms clearly articulate our security & privacy commitments to customers. We have evolved these terms over the years based on feedback from our customers and regulators. Core to this is the understanding that any data that a customer puts into our systems will only be processed in accordance with the customer's instructions.

Google Cloud also commits to take security measures to ensure the confidentiality, integrity and availability of our systems. These are laid out in some detail in the agreement along with a further commitment that any changes we make to our security measures going forward will not degrade security. Our goal in stating this is to provide our customers continuous security improvement.

The table below shows the SLAs for some of the services in Google Cloud and Google Workspace. The SLAs for all services are published in the Google Cloud Service Level Agreement, allowing you to verify whether each Google Cloud service meets your service requirements. The table below reflects that status as of October 2024. For the latest information, please refer to the links for each service.

Google Cloud services	Eligible Services	Monthly uptime guaranteed by SLA
Compute Engine	Instances in Multiple Zones	99.99%
	A Single Instance of the Memory Optimized family	99.95%
	A Single Instance of all other families	99.9%
Cloud Storage	Standard storage class in a multi-region or dual-region location of Cloud Storage	99.95%
	Standard storage class in a regional location of Cloud Storage; Nearline, Coldline, or Archive storage class in a multi-region or dual-region location of Cloud Storage	99.9%
	Nearline, Coldline, or Archive storage class in a regional location of Cloud Storage; Durable Reduced Availability storage class in any location of Cloud Storage	99.0%
Cloud SQL	Cloud SQL Enterprise Plus edition with high availability (HA)	99.99%

	Cloud SQL Enterprise edition with high availability (HA)	99.95%
Cloud Functions	-	99.95%
Google Kubernetes Engine	Zonal cluster (control plane)	99.5%
	Regional cluster (control plane)	99.95%
	Autopilot cluster (control plane)	99.95%
	Autopilot Pods in Multiple Zones	99.9%
	GKE Enterprise Autopilot Pods in Multiple Regions	99.99%

Table 2: SLA for selected Google Cloud services

Google Workspace Services	Eligible Service	Monthly uptime guaranteed by SLA
Google Workspace	AppSheet applicable services (※1)	99.99%
	Google Workspace applicable services (※2)	99.99%

Table 3: Google Workspace Service SLA

*1: AppSheet eligible services
AppSheet Enterprise Standard (purchased before June 17, 2024), AppSheet Enterprise Plus
*2: Google Workspace eligible services
Gmail, Google Calendar, Google Cloud Search, Google Docs, Google Spreadsheets, Google Slides, Google Forms, Google Drive, Google Groups for Business, Google Chat, Google Meet, Google Keep, Google Sites, Google Jamboard, Google Tasks, Google Vault, Google Voice

Security and Compliance

Google Cloud and Google Workspace undergo several independent third party audits to test for data safety, privacy, and security. Our third party audit approach is designed to be comprehensive in order to provide assurances of our level of information security with regard to confidentiality, integrity and availability. Customers may use these third party audits to assess how Google's products can meet their compliance and data-processing needs.

As a provider of cloud services to Agencies, Google complies with Information system Security Management and Assessment Program (ISMAP). Google's cloud services, including Google Cloud and Google Workspace, are registered as ISMAP certified cloud services. Please check

the ISMAP Cloud Service List for details of Google services and products that are ISMAP registered.

Other major third-party certifications that Google has obtained and complies with are listed below. For more information see our Compliance Resource Center.

ISO/IEC 27001
ISO/IEC 27001 is a security standard that outlines and provides the requirements for an information security management system. The 27001 standard lays out a framework and checklist of controls that allow Google to ensure a comprehensive and continually improving model for security management. Google Cloud and Google Workspace arecertified as ISO 27001 compliant.

ISO/IEC 27018
ISO/IEC 27018 is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google Workspace and Google Cloud are certified as ISO/IEC compliant.

ISMAP
Information system Security Management and Assessment Program (ISMAP) is a government-led program to evaluate and register cloud services that meet government security requirements. ISMAP is based on ISO27001, ISO27002, ISO27017, government uniform standards, and NIST SP 800-53. Google Workspace and Google Cloud completed the assessment for ISMAP compliance and are registered as an ISMAP compliant Cloud Service Provider. Registration details can be confirmed on the Information Technology Promotion Agency (IPA) website.

NIST SP 800-171
NIST SP 800-171 is a security standard for maintaining the confidentiality of controlled unclassified information (CUI) in non-federal information systems and organizations. The security controls in NIST SP 800-171 can be linked to NIST SP 800-53, and Google Cloud services have already undergone an independent third-party assessment to determine compliance with the NIST SP 800-53 controls that are in scope for FedRAMP, as well as all control requirements outlined in NIST SP 800-171. The services that are subject to the NIST SP 800-171 third-party assessment can be found on the Google Cloud website.

Endpoint

In order to securely handle information, one must access that information using a secure endpoint. At Google, we have developed browser and OS technologies as part of the Chrome product family. These products have a very small attack surface in order to prevent common

threats from taking hold on an endpoint. These solutions are available to our customers as Chrome Browser, Chrome OS and ChromeBooks centrally managed by Chrome Enterprise.

Chrome Browser is a minimal browser that automatically updates itself. It uses SafeBrowsing to check URLs against a database of known bad URLs and can warn or block sites that are deemed high risk. Chrome tabs are sandboxed. Even I-frames in a tab are sandboxed. Chrome itself is isolated on the OS and has no access to other processes.

ChromeBook runs Chrome OS. Chrome OS is a read-only OS so malware has no way to infect or change the system files. ChromeBook maintains 2 copies of Chrome OS; a working copy and a standby copy. Failure to boot the working copy will pull up the standby copy. This is beneficial for upgrades which are done on the standby copy and then it becomes the working copy on reboot. So, not only do you get security, but you get no downtime for upgrades. ChromeBooks have a Titan-C chip that will verify the firmware, OS and browser code. Should it detect a change it will not boot that version of the OS.

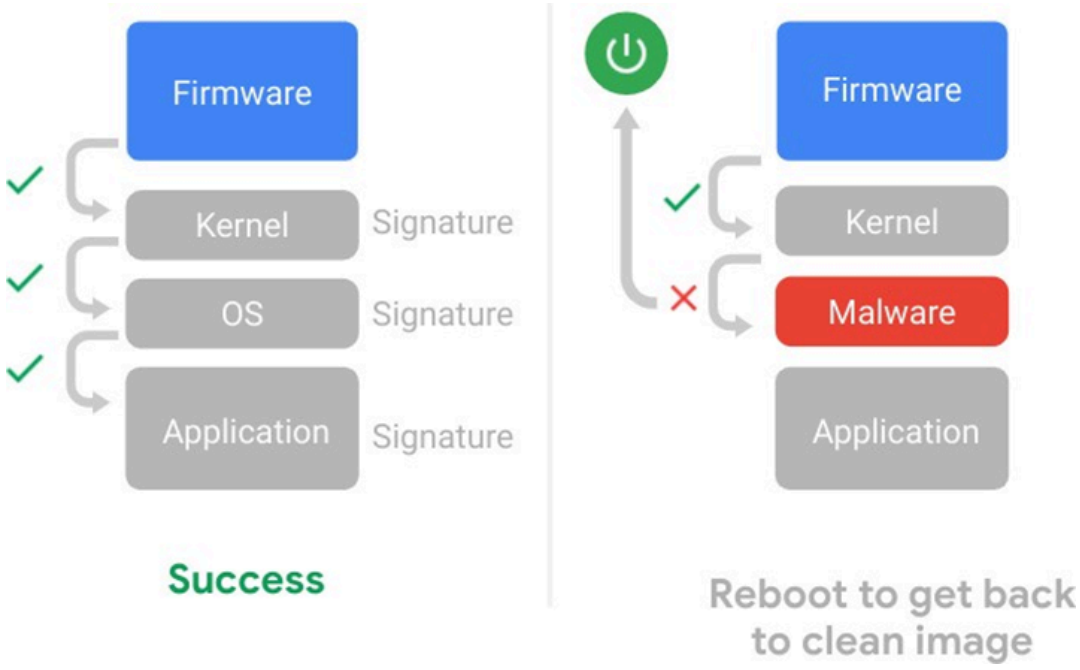


Figure 3: Verification by a Titan-C chip

ChromeBook encrypts data at rest but Chrome users store a very small amount of data on their Chromebook since most of their data is in Google Cloud Services and Google Workspace. Thus, there is minimizing the risk of ransomware.

Chrome Enterprise Upgrade is a cloud based management system for having consistent administration over the Chrome OS environment. Software deployment, upgrades and Chrome settings can be configured for your entire fleet from one single console.

Google Cloud

Identity

Identity is the backbone of access control. Google Cloud supports multiple identity providers as well as our own Cloud Identity.

Cloud Identity uses machine learning to detect unauthorized access and can even detect and block unauthorized intruders using the correct password.

Cloud Identity also supports the strongest forms of account protection including multiple 2FA options such as FIDO compliant security keys. Googlers use security keys when logging into their Google accounts to provide stronger identity protection and to prevent phishing attacks. We recommend our customers do the same.

Access Controls

In Google Cloud, to handle information securely, it is important to set appropriate permissions to access information to the minimum extent necessary. In Google Cloud, all services require authentication to be used. Authentication is primarily managed by Identity and Access Management (hereinafter referred to as "IAM"). IAM allows you to grant roles to members such as users and groups. These roles are made up of fine-grained permissions. Carefully selected roles are provided in advance, and you can also create custom roles as needed.

Conditions (IAM Conditions) can also be applied to roles. So for example a contractor that is only supposed to work 9 to 5 can have a condition added to the roles attached to them that limits their access to just 9 to 5.

Google Cloud has a resource manager where you can set up a folder tree to organize your projects. Access controls can be managed at any layer of the hierarchy and inherited down which is beneficial for good governance. Folders dedicated to specific information could be established and access controls applied there so as to have them consistent across all projects in that folder.

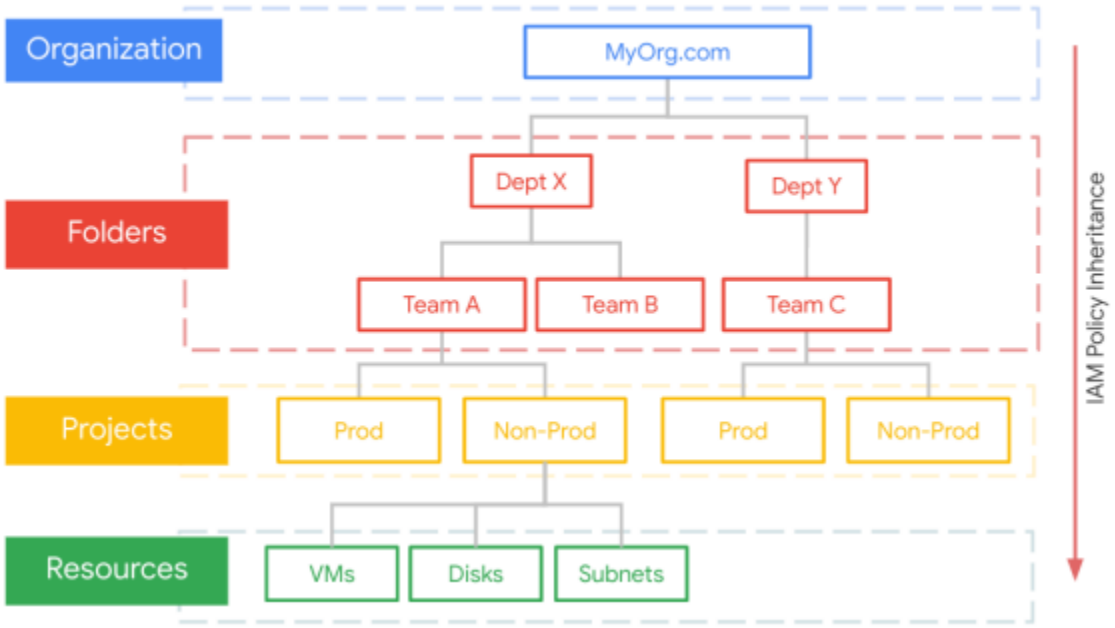


Figure 4: Relationship between a folder tree and Inheritance of IAM Policy

One of the biggest challenges for enterprise customers is not granting access but rather taking it away when it is unnecessary or excessive. IAM Recommender uses machine learning to see what permissions are being used and which are not and then makes recommendations to remove excess access. Policy analyzer can help you figure out who has access to what, which is helpful in an audit situation.

Some Google Cloud services include service specific access controls that exceed what IAM can offer. For example in BigQuery you can set up limited views of data tables and you can filter rows and columns meeting certain criteria. This can be very useful for minimizing the data analysts can see or filtering it out entirely.

In Google Workspace you can apply access controls on services based on the context of the user's identity and device. You can define at the file level who can read, comment, or edit each individual file or folder.

Network Access Controls

In a traditional network, including most cloud providers, firewall rules for network access control can only be applied at choke points. In Google Cloud firewall rules are much more flexible. They can be applied to a single VM, tagged assets, assets that share the same service account or a combination of factors.

Instead of applying the same rules to every project, common rules can be applied across projects at folder or organization level using hierarchical firewall policies.

The rules affecting an asset can be analyzed both from the command line as well as in the Network Intelligence Center.

It is also important to control access to service APIs. In Google Cloud you determine what APIs you want to turn on or off. Furthermore, you can place a perimeter around the APIs of your project using VPC Service Controls. VPC-SC can block data egress and place conditions on ingress.

Proper management of DNS is also important to protect your domains against spoofing and cache poisoning attacks. DNSSEC is a feature of the Domain Name System (DNS) that authenticates responses to domain name lookups. Cloud DNS supports DNSSEC, and while it does not provide privacy protection for these lookups, it prevents responses to DNS requests from being tampered with or poisoned.

Application Access Controls

Google Cloud provides the infrastructure for our customers to build their applications. The access controls inside those applications are part of the application logic the customer provides. However the access to those applications can leverage our context aware access system called Chrome Enterprise Premium.

Chrome Enterprise Premium is a zero-trust solution provided through Google's global network, enabling secure access to applications and cloud resources by protecting data from centralized threats. Zero trust is a security model used to protect organizations based on the concept that people and devices are not trusted by default, even if they are within the organization's network. The zero-trust approach aims to eliminate implicit trust by enforcing strict identity authentication and authorization not just at the trusted perimeter, but throughout the entire network.

Chrome Enterprise Premium allows you to define which users can access which applications under which conditions. Those conditions can be related to the situation (e.g. time), the device (e.g. corporate managed) and the user’s identity and authentication (e.g. MFA). This adds stronger controls that simple identity to systems with important information.

Chrome Enterprise Premium also has the ability to examine data uploads/downloads in Chrome and determine if certain data is included. It can then take a predefined action such as to block that data movement.

Google Cloud

Logging

Google Cloud offers extensive audit logging for services. Network logs provide both network and security operations with in-depth network service telemetry. VPC Flow Logs can be used for network monitoring, forensics and real-time security analysis. Packet level capture can be done with Packet Mirroring for content analysis or to feed into a Network Intrusion Detection System. Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules. NAT and DNS logs are also available for threat analysis.

Google Cloud has Cloud Audit logging to log API activities including who did what, where, and when. Data access logs can provide additional details at the data level and are especially useful for data management services.

Google cloud does not handle customer data but if a customer specifically instructs us to access their data as part of support troubleshooting then that access is also logged and those logs can be made visible to customers via Access Transparency.

Cloud Operations provides a centralized tool for logging that can take in logs from a multitude of sources including custom logs sent from OS level agents, Fluentd, REST APIs, client libraries or 3rd party applications. Logs can be investigated and analyzed in real time with Log Viewer.rIn addition, you can visualize and alert on your logs with logs-based metrics and Cloud Monitoring.

Google Cloud provides a variety of log storage and retention options to meet both security & compliance requirements. System logs and data access logs are retained for 30 days by default or optionally up to 10 years. Admin logs are retained for 400 days in locked storage. Log data is immutable, encrypted at rest, and monitored via Access Transparency.

Google Workspace includes extensive logging capabilities for everything from administration to users to services to devices. These logs can be fed to Cloud Operations in Google Cloud for consolidated analysis.

Threat Detection

Security Command Center (SCC) in Google Cloud provides wing to wing risk management for Google Cloud customers. One component of SCC is threat detection. SCC will compare logs to known indicators of compromise as well as suspicious behaviors and surface alerts. Those alerts can be acted on automatically by triggering cloud functions. So for example, a VM detected to be compromised could be imaged and isolated on the network all automatically.

Logs can also be exported from Google Cloud to Google Security Operations SIEM or 3rd party SIEMs like Splunk for further threat analysis or correlation with non-cloud logs to see the bigger enterprise threat picture. Google Security Operations SIEM continuously compares all your logs to a huge database of indicators of compromise (IOC) and surfaces any matches. Google Security Operations SIEM can search petabytes of logs in a single second.

Google Security Operations SOAR is a platform designed to help organizations detect, investigate, and respond to security threats in real time. Google Security Operations SOAR leverages Google's machine learning capabilities to automate and streamline security workflows, allowing security analysts to investigate incidents, create workflows, and automate response actions without requiring advanced coding knowledge.

Managed Services

Maintaining systems is complicated, costly and distracting for most customers. We recommend using managed services which we maintain for you. As you can see by the diagram below the more managed a service is the more you can focus on your data and leave the responsibility for the underlying infrastructure to Google (Shared Responsibility Model).

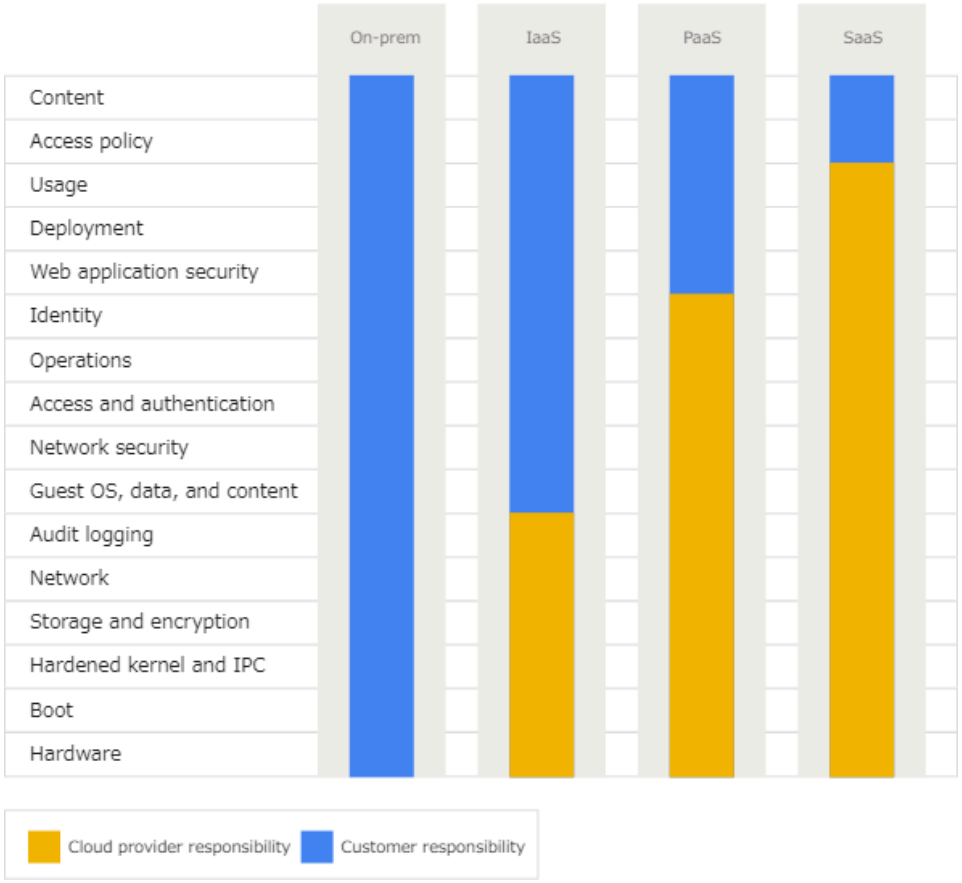


Figure 5: Responsibilities that Google and Customer have in Google Cloud

Even in cases where compute services are required, we recommend taking advantage of the most managed form. For example a simple function can be run in Cloud Functions without any need for further management. Containers can be managed in GKE with node auto-upgrades which decreases the maintenance burden.

The team that manages the security of GKE is the same team that designed and wrote large parts of K8s identity, authorization, and security policy code. The same team that led or contributed to the investigation, triage, patching, and notification of every serious K8s vulnerability since day 0.

Secure CI/CD Pipeline

One way a threat actor might abuse information is to alter the code that is loaded into an application handling information. This is why having security as part of your continuous integration and delivery pipeline (CI/CD) is so important. We recommend having a healthy

code review process in place and have provided a guide to the public where we share our own practices and thoughts on this subject.

Google Cloud provides COS (Container Optimized OS) for nodes. Container-Optimized OS's small OS footprint minimizes security exposure while still containing essential built-in security features like a minimal read-only root file system, file system integrity check, locked-down firewall, and audit logging. Automatic updates patch security vulnerabilities for you and in a timely manner, further reducing your risk of compromise.

Shielded GKE Nodes is built on hardware with a Titan chip that sets off a provenance validation sequence from host bootloader right up to the guest COS kernel in order to ensure end to end supply chain security.

Ensuring vulnerable containers are detected and addressed is key. Google Cloud can scan your containers added to Artifact Registry and report any defects.

Container policies can be set using Anthos Container Policy Controller. This is great for governance and can be used to ensure that a project team doesn't deploy containers with rights exceeded that allowed by company policy.

Using Binary Authorization it is possible to define signatures for passing various steps of the CI/CD pipeline and these signatures can be checked as a condition of deployment. This not only ensures all steps were passed but also keeps unauthorized code from being deployed to production.

Risk Detection

Application code can also be checked while running by Web Security scanner which looks for common misconfigurations and vulnerabilities targeted by OWASP. Our premium offering even scans Google Cloud looking for web applications and can surface shadow applications that may have been built without authorization.

Security Command Center checks your entire Google Cloud organization for misconfigurations and vulnerabilities and then maps those against a list of your cloud assets. In fact SCC will map risks and threats not only to assets but also to different compliance frameworks such as ISO 27001, PCI DSS and the CIS best practices for Google Cloud. This allows you to meet your obligations to prevent and detect incidents affecting information you place in Google Cloud. Additionally, Google Cloud Security Best Practices Center provides best practices for achieving security and compliance goals when deploying workloads on Google Cloud, allowing customers to implement measures to prevent configuration errors..

In Google Workspace you can get insights into security events and metrics that demonstrate your security effectiveness in a single, comprehensive dashboard called Security Center. From

there you can Identify, triage, and take action on security and privacy issues such as deleting malicious emails across your organization and examining file sharing to spot and stop potential data exfiltration.

Data Governance

Keeping track of important information can be a challenge for organizations as different systems and functions in the company make different copies. Data Governance is key and Google Cloud can help with this. By data governance we mean:

1. Discover information
2. Label information
3. Apply rules to information

Data Catalog can use DLP API to find and apply metadata labels to your information regardless of its location. Those labels can be used to apply rules so as to screen in/out certain data in processing jobs or data analytics systems.

Customers can select the region to run their workloads including two regions under Japanese jurisdiction.

Google Workspace also has DLP capabilities which administrators can configure to detect PII in files and take actions such as alerts or set restrictions on them such as to restrict outside sharing.

Data Transformation

Information can be hidden or removed at different handling points using transformation techniques. DLP API can remove PII by masking or redacting the PII.

ID	Job Title	Phone	Comments
359740	Senior Engineer	307-964-0673	Please email them at jane@imadethisup.com
981587	VP, Engineer	713-910-6787	none
394091	Lawyer	692-398-4146	Updated phone to: 692-398-4146
986941	Senior Ops Manager	294-967-5508	none
490456	Junior Ops Manager	791-954-3281	Tried to verify account with their SSN 222-44-5555

ID (FPE)	Job Title	Phone	Comments
438422	Engineer	307-###-####	Please email them at [Found Email]
530375	Engineer	713-###-####	none
496534	Lawyer	692-###-####	Updated phone to: 692-###-####
242348	Ops	294-###-####	none
593887	Ops	791-###-####	Tried to verify account with their SSN [Found SSN]

Table 4 : Masking the PII by DLP API

There may be times when you both need to use PII but also need to hide the PII. There are two ways to do that. In the case of using it as a field in a data table you can use DLP API to replace the PII with unique tokens (tokenization). If you only need to hide the data in storage or transit but would like to unhide it later then encryption makes more sense.

Google Cloud offers many encryption options. Cloud Key Management Service (Cloud KMS) can have cryptographic operations as a managed service that you access via an API. Additionally, you can manage customer-managed encryption keys (CMEK) with Cloud KMS, allowing you to own and control the keys used to protect your data stored on Google Cloud..

Under Cloud HSM you can use the same KMS front end knowing the backend is a FIPS-2 Level 3 certified HSM. Depending on your security requirements, you can also use your own encryption keys. In fact, you can even use the Cloud KMS front end with an External Key Manager if you wish to separate duties.

Data Deletion

Customer data in Google Cloud belongs to the customer and the customer can select to delete it at any time. Doing so makes the data immediately unavailable and kicks off wipe out procedures that extend to the various service components involved. These wipe out procedures can take up to 180 days. These procedures once complete provide for irreversible destruction of the data. Details are in the following whitepapers for Google Cloud & Google Workspace.

Backup and Resilience

It is necessary to establish operational continuity plans for information systems and perform backups in order to continue the business operations of the organization in the event of an emergency. By using backup and disaster recovery solutions on Google Cloud, you can prepare for various threats or failures that lead to data loss.

Google Cloud products and services offer a broad range of data protection features such as Backup for GKE, Persistent Disk snapshots, Cloud SQL backups, Filestore backups, and geo-redundant Cloud Storage. You can also create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems.

Backup and DR Service protects a broad spectrum of workloads and manages them from a central dashboard. It also serves critical use cases such as recovery from data corruption, data loss, ransomware recovery, or database cloning for test/dev.

We design the components of our platform to be highly redundant to prevent data loss on the infrastructure managed by Google as a cloud service provider. Our data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption.

Our systems are designed to minimize downtime or maintenance windows for when we need to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from the initial design through to ongoing operations, see Google Cloud infrastructure reliability guide.

In addition, Google Cloud Service Health Dashboard (CSH) displays status information for products included in Google Cloud. The status includes informational messages about interruptions, outages, and temporary issues. This allows customers to understand ongoing incidents, identify the causes of system failures built on Google Cloud, and organize the estimated time for recovery.

Managing Third Party Suppliers

In cases where a cloud service provider subcontracts its services, Agencies should be careful to ensure that the service provider appropriately manages third-party suppliers.

For most data-processing activities, we provide our services in our own infrastructure. However, we may engage some third-party suppliers to provide services related to Google Cloud, including customer support and technical support.

Before outsourcing a supplier, we assess their security and privacy practices. This assessment checks whether the supplier provides a level of security and privacy that is appropriate for their access to data and for the scope of the services that they are engaged to provide. After we have assessed the risks that are presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

For more information, see the Supplier Code of Conduct.

Training & Consultation

Google Cloud has a wide range of training and consultation support for our customers such as:

- Pre-sales staff to walk you through our services and help choose the right ones
- Training and education staff to train your team
- Cloud on Air and Youtube Videos
- Online training partners so you can train on your own schedule
- Certification programs to level set on required skills
- Online documentation in multiple languages
- Google Cloud Skills Boost to practice using our services
- Post-sales consulting services
- System integrator partnerships to build and manage solutions at scale
- A lively online community of blogs, knowledge, videos and chat rooms to share ideas and derive inspiration

Partner Solutions

Google Cloud has partnered with a wide variety of security solutions companies to make their solutions available to our customers either via the Google Cloud Marketplace or other partnership agreements. In addition we provide basic compute services that can support most security solutions regardless of whether they are a Google Cloud partner or not.

Our sales team is happy to hear your security requirements and provide consultation on which partner solutions best match your use cases.