National Cyber Security Centre (NCSC) Cloud Security Principles

Google Cloud Mapping

This document is designed to provide guidance for public sector and enterprise organisations ("**regulated entity**") by the National Cyber Security Centre (**"NCSC"**) to consider Cloud Security Principles ("**framework**") in the context of Google Cloud Platform ("**GCP**") and the Google Cloud Services Contract.

We focus on the following requirements of the framework: Cloud Security Principles 1 - 14. For each paragraph, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Services Contract.

In the pre-cloud IT model, organisations maintained full responsibility for their environment. They managed everything from the networking and infrastructure to the security controls and applications. In the cloud IT model, management of the IT environment, including responsibilities for security and compliance, is shared between the customer and its cloud service provider. This is often referred to as the Shared Responsibility Model. Google Cloud Platform's part in the shared responsibility model includes providing services on a highly secure and controlled platform offering a wide array of security features customers can benefit from. Shared responsibility enables our customers to allocate resources more effectively to their core competencies and concentrate on what they do best. The shared responsibility model does not remove the accountability and risk from customers using Google Cloud Platform services, but it does help relieve the burden as we manage and control system components and physical control of facilities; it also shifts a portion of the cost of security and compliance onto Google Cloud Platform and away from our customers. The different responsibilities held by Google Cloud Platform and its customers are discussed in further detail in our Google Cloud securities foundations guide.

Terms

- Alpha - refers to a service that is in alpha at the time this document is published. Follow the links provided to understand the current release status of the service.
- Beta - refers to a service that is in beta at the time this document is published. Follow the links provided to understand the current release status of the service.
- Services - refers to Google Cloud services that you use to provide a solution on the platform.

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
1	**Principle 1: Data in Transit Protection**		
2	User data transiting networks should be adequately protected against tampering and eavesdropping. This should be achieved through a combination of:		
3	1. network protection - denying your attacker the ability to intercept data	Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Data in transit inside a physical boundary controlled by or on behalf of Google is generally authenticated. Additionally, Google has implemented network and host based tools to detect and respond to potential security incidents. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves: • Tightly controlling the size and make-up of Google's attack surface through preventative measures • Employing intelligent detection controls at data entry points; and • Employing technologies that automatically remedy certain dangerous situations. For our customers, Google provides detailed information about our security practices so that customers can understand them and consider them as part of their own risk analysis.	Data Security; Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our trust and security resources page Please review Google Infrastructure Security Design Overview | Solutions regarding defense-in-depth techniques deployed across our infrastructure.	
4	2. encryption - denying your attacker the ability to read data	Security by default At Google, we take the following proactive steps to assist you: **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: Encryption at rest in Google Cloud. **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Google uses encryption in transit to protect your data being intercepted while data moves between your site and the cloud provider or between two services. This protection is achieved by encrypting the data before transmission; authenticating the endpoints; and decrypting and verifying the data on arrival. For example, Transport Layer Security (TLS) is often used to encrypt data in transit for transport security, and Secure/Multipurpose Internet Mail Extensions (S/MIME) is used often for email message security. More information is available at: Encryption at transit in Google Cloud. In addition, Google offers tools you can choose to use these encryption and key management tools: ● Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises. ● Cloud HSM lets you protect Cloud KMS encryption keys and perform cryptographic operations within a managed hardware security module. You can generate, use, rotate, and destroy various symmetric and asymmetric keys.	Data Security; Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		● See using Cloud KMS with other products to understand which products are supported with the service, i.e. Cloud SQL. Google also publishes articles such as Exploring container security: Use your own keys to protect your data on GKE to provide further guidance to customers for securing their solutions. ● Google Cloud Key Management (beta) lets you protect data at rest using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure. The service currently supports BigQuery and Compute Engine. See use third-party keys in the cloud with Cloud External Key Manager. ● Key Access Justification (alpha) works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set. See Key Access Justifications: a new level of control and visibility.	
5	**Principle 2: Asset Protection and Resilience**		
6	**2.1 Physical location and legal jurisdiction**		
7	In order to understand the legal circumstances under which your data could be accessed without your consent you must identify the locations at which it is stored, processed and managed. You will also need to understand how data-handling controls within the service are enforced, relative to UK legislation. Inappropriate protection of user data could result in legal and regulatory sanction, or reputational damage.	Locations To provide you with a fast, reliable, robust and resilient service, Google may store and process your data in Google or its subprocessors facilities, however, Google provides you with the ability to choose where to store your data. Once you choose a specific region, Google will not store it outside your chosen region(s). ● Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page. ● Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy on Google Cloud Whitepaper. Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:	Data Location (Service Specific Terms)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		- The same robust security measures apply to all Google facilities, regardless of country / region. - Google makes the same commitments about all its subprocessors, regardless of country / region. Use of your information Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. Privacy and Non-Public Personal Information Google will comply with privacy laws and regulations applicable to it in the provision of the Services. In addition, you can define additional controls through organisation policy service. The 'Resource Location Restriction' constraint defines the set of locations where location-based GCP resources can be created. Identity Access Management security controls allows you to define who can create resources in your organisation.	Protection of Customer Data Processing of Data; Roles and Regulatory Compliance (Cloud Data Processing Addendum)
8	**2.2 Data Center Security**		
9	Locations used to provide cloud services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding data center and network security and data security. Google anticipates physical threats to its data centers and has implemented countermeasures to prevent or limit the impact from these threats. Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control systems that are linked to a system alarm. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on an individual's job responsibilities. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to help cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site through digital video recorders 24 hours a day, 7 days a week. For more information on Google data centers refer to below:	Data Security; Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		● Appendix 2 of Google Cloud's Cloud Data Processing Addendum describe the security measures that Google will implement and maintain. ● Google Cloud Security White Paper for details on our data center security. ● Information on our Data Center Security page ● Please review Google Infrastructure Security Design regarding defense-in-depth techniques deployed across our infrastructure.	
10	**2.3 Data at Rest Protection**		
11	To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service should be protected regardless of the storage media on which it's held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.	Data Center Security Refer to Row 4 for more information about encryption at rest and Row 9 for data center security. Data Backup Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup. Google will comply with all national data protection regulations applicable to it in the provision of the Services. In addition, Google makes commitments to protect your data, including regarding security, access and transfer in the Cloud Data Processing Addendum.	Protection of Data (Cloud Data Processing Addendum)
12	**2.4 Data Sanitization**		
13	The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data. Inadequate sanitisation of data could result in: 1. your data being retained by the service provider indefinitely 2. your data being accessible to other users of the service as resources are reused 3. your data being lost or disclosed on discarded, lost or stolen media	Deletion On termination of the contractual relationship, Google will comply with your instruction to delete customer data from Google systems. Google has strict policies and procedures to 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 the appropriate operations manager before release. For more information, please see: data deletion on GCP, media sanitization process and the decommissioned disks and disk erase policy in the Cloud Data Processing Addendum.	Deletion on Termination (Cloud Data Processing Addendum) Security measures (Cloud Data Processing Addendum)
14	**2.5 Equipment disposal**		

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
15	Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.	Refer to Row 13 for more information on equipment disposal.	N/A
16	**2.6 Physical Resilience and Availability**		
17	Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business.	Google Availability and Resilience Google embeds redundancy as part of its architecture and failure is expected and corrected continuously. Google's highly redundant infrastructure also helps protect our customers from data loss. For more information, refer to our Reliability Architecture Framework. Google Cloud services are available in locations across North America, South America, Europe, Asia, and Australia. These locations are divided into regions and zones. You can choose where to locate your applications to meet your latency, availability, and durability requirements. Refer to our whitepaper on Infrastructure design for availability and resilience for more details. Under the shared responsibility model, certain architectural decisions made by the customer can impact the availability of workloads on GCP. Detailed guidance is available for each service to enable customers to design and implement appropriate levels of availability in their deployments - see example below: ● Using load balancing for highly available applications Additionally, the SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. Furthermore, Google provides our customers with tools you can choose to use these networking tools provided by Google: ● Cloud Load Balancing provides scaling, high availability, and traffic management for your internet-facing and private applications. ● Dedicated Interconnect is a high-performance option providing direct physical connections between your on-premises network and Google's network.	Service Level Agreements (Cloud Data Processing Addendum)
18	**Principle 3: Separation Between Users**		
19	A malicious or compromised user of the service should not be able to affect the service or data of another.	Google makes commitments to protect your data, including regarding security, access and transfer in the Cloud Data Processing Addendum.	Security Measures; Data Storage, Isolation and Logging (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		To keep data private and secure, Google logically isolates each customer's data from that of other customers. 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 APIs solely to a specific whitelist of other services. That 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 services can be similarly configured to allow or deny their accesses. All of these types of identities (machine, service, and employee) are in a global namespace that the infrastructure maintains. End user identities are handled separately. Refer to Google's inter-service management Google Infrastructure Security Design Overview - Inter-service Access Management for more information. Ownership You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications. See Google Enterprise Privacy Commitments.	Intellectual Property (Cloud Data Processing Addendum)
20	**Principle 4: Governance framework**		
21	The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined. Having an effective governance framework will ensure that procedure, personnel, physical and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments and the appearance of new threats.	Google recognizes that regulated entities need to review our internal controls, systems and data security and privacy protections for the services as part of their risk assessment. To assist, Google undergoes several independent third-party audits on at least an annual basis to provide independent verification of our operations and internal controls. Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • ISO/IEC 27701:2019 (PII) • PCI DSS • SOC 1 • SOC 2 • SOC 3 Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS and evidence of its effectiveness is provided via ISO/IEC 27001 certification.	Certifications and Audit Reports (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		You can review Google's current certifications and audit reports at any time. - Google's ISO certifications are available on our Compliance Resource Center. - Google's SOC reports and PCI Attestation of Compliance (AOC) are available to customers under NDA and can be requested from your Google Cloud account representative.	
22	**Principle 5: Operational Security**		
23	**5.1 Configuration and Change Management**		
24	You should have an accurate picture of the assets which make up the service, along with their configurations and dependencies.	This is a customer consideration. Google provides following tools to assist you for configuration management: - Security Command Centre assists you with identifying security misconfigurations and compliance violations in your Google Cloud assets and resolves them by following actionable recommendations. - Resource Manager allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. See Enterprise resource best practices guidance for further information - Cloud Deployment Manager is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. Customers can also use third party tools such as Terraform to manage their environments on GCP.	N/A
25	Changes which could affect the security of the service should be identified and managed. Unauthorised changes should be detected.	This is a customer consideration. Refer to row 24 for more information about tools provided to customers to manage and monitor configuration changes. Additionally, customers are able to validate the full hosting stack - including hardware, firmware and hypervisor - using Shielded VMs, which enable live measurement, monitoring, and alerting for any changes of the full stack. Google also provides customers with robust logging services that can be configured to meet customer security requirements. Audit Logging	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		Cloud Audit Logs provides the following audit logs for each Cloud project, folder, and organization: ● Admin Activity audit logs ● Data Access audit logs ● System Event audit logs ● Policy Denied audit logs Google Cloud services write audit log entries to these logs to help you answer questions such as "who did what, where, and when?" within your Google Cloud resources.	
26	Where change is not effectively managed, security vulnerabilities may be unwittingly introduced to a service. And even where there is awareness of the vulnerability, it may not be fully mitigated.	This is a customer consideration. Google offers our tools and services to our customers to assist with deploying management guardrails to help avoid erroneous configuration. For example: ● Cloud Logging - Supported across Google Cloud services and integrated with Cloud Monitoring, Error Reporting, and Cloud Trace so you can quickly troubleshoot issues across your infrastructure and applications. ● Anthos Config Management - With Anthos Config Management, you can create a common configuration across all your infrastructure, including custom policies, and apply it both on-premises and across clouds. Anthos Config Management evaluates changes and rolls them out to all Kubernetes clusters so that your desired state is always reflected. ● OS config management (beta) - You can use the OS configuration management service to deploy, query, and maintain consistent configurations (desired state and software) for your VM instance (VM).	N/A
27	**5.2 Vulnerability Management**		
28	Service providers should have a management process in place to identify, triage and mitigate vulnerabilities. Services which don't, will quickly become vulnerable to attack using publicly known methods and tools.	Google's vulnerability management team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The vulnerability management team tracks such issues and follows up frequently until they can verify that the issues have been remediated. Google administrates a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews and external audits. Refer to our security whitepaper on security monitoring and vulnerability management.	
29	**5.3 Protective Monitoring**		
30	A service which does not effectively monitor for attack, misuse and malfunction will be unlikely to detect attacks (both successful and unsuccessful). As a result, it will be unable to quickly respond to potential compromises of your environments and data.	Google Monitoring Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open-source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. 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. Automated network analysis helps determine when an unknown threat may exist and escalates to Google security staff, and network analysis is supplemented by automated analysis of system logs. Security products In addition to the tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. See Google Cloud Security and Identity page for further information about the tools. Information. Here are some examples: ● Cloud Identity and Access Management helps to prevent unauthorized access by controlling access rights and roles for Google Cloud Platform resources.	Ongoing Performance Monitoring

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		- Cloud Security Scanner automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities. - Event Threat Detection automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment. - Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems. - Shielded VMs enable live measurement, monitoring, and alerting for any changes of the full stack. Performance reports You can monitor Google's performance of the Services (including the SLAs) on a regular basis using the functionality of the Services. For example: - The Google Cloud Status Dashboard provides status information on the Services. - Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. - Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).	
31	**5.4 Incident Management**		
32	Unless carefully pre-planned incident management processes are in place, poor decisions are likely to be made when incidents do occur, potentially exacerbating the overall impact on users. These processes needn't be complex or require large amounts of description, but good incident management will minimise the impact to users of security, reliability and environmental issues with a service.	Google has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it 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 guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling	Data Incidents (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		evidence 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 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Incidents & the Google Cloud dashboard page. Security breaches Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper.	
33	**Principle 6: Personnel Security**		
34	Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel. The service provider should subject personnel to security screening and regular security training. Personnel in these roles should understand their responsibilities. Providers should make clear how they screen and manage personnel within privileged roles	Company principals Information about Google Cloud's leadership team is available on our Media Resources page. Employee background checks Before they join our staff, Google will verify an individual'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. 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.	Personnel Security; Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		Internal security and privacy events Google hosts regular internal conferences to raise awareness and drive innovation in security and data privacy, which are open to all employees. Security and privacy is an ever-evolving area, and Google recognizes that dedicated employee engagement is a key means of raising awareness. One example is "Privacy Week," during which Google hosts events across global offices to raise awareness of privacy in all facets, from software development, data handling and policy enforcement to living our privacy principles. Google also hosts regular "Tech Talks" focusing on subjects that often include security and privacy.	
35	**Principle 7: Secure Development**		
36	Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.	The security of a cloud service consists of two key elements: Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: • Our infrastructure security page • Our security whitepaper • Our cloud-native security whitepaper • Our infrastructure security design overview page • Our security resources page In addition, you can review Google's SOC 2 report. The focus of this report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy.	Data Incidents (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		Security of your data and applications in the cloud You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services. (a) Security products In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Google Cloud Security and Identity page page. (b) Security resources Google also publishes guidance on: ● Security best practices ● Security use cases, (i.e. how do I configure a secure by design environment for my cloud deployments).	
37	**Principle 8: Supply Chain Security**		
38	The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement. Cloud services often rely upon third party products and services. Consequently, if this principle is not implemented, supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	Google works with third parties to support our business and operations. Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you and will remain liable to you for any subcontracted obligations. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will: ● provide information about our subcontractors (including their function and location); ● provide advance notice of changes to our subcontractors; and ● give regulated entities the ability to terminate if they have concerns about a new subcontractor. For more information around Google's supply chain efforts, refer to our Responsible Supply Chain report.	Google Subcontractors

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
39	**Principle 9: Secure User Management** Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.		
40	**9.1 Authentication of users to management interfaces and support channels**		
41	In order to maintain a secure service, users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the service. These activities may be conducted through a service management web portal, or through other channels, such as telephone or email. They are likely to include such functions as provisioning new service elements, managing user accounts and managing consumer data. Service providers need to ensure that all management requests which could have a security impact are performed over secure and authenticated channels. If users are not strongly authenticated then an imposter may be able to successfully perform privileged actions, undermining the security of the service or data.	This is a shared responsibility between Google and the customer. Authenticated Users Google maintains policies and procedures that enforce data access permissions. Two factor authentication is required for all employee access to all company and customer resources. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. Additionally, Google native authentication requires a minimum 8 character complex password. Tenants can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the tenant, who can decide to force a password change on any user that is later detected to have a password that is weak. Google's native authentication has protections in place that would detect a brute force attack and challenge the user to solve a Captcha and would auto lock the account if suspicious activity is detected. The tenant's System Administrators can reset that account for the end user. Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. For more information refer: Encryption in Transit in Google Cloud. For customers, Google offers our tools and services such as Cloud Identity and Access Management which helps to prevent unauthorized access by controlling access rights and roles for Google Cloud Platform resources.	Data Security; Security Measures (Cloud Data Processing Addendum)
42	**9.2 Separation and access control within management interfaces**		
43	Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If users are not adequately separated within management interfaces, one user may be able to affect the service, or modify the data of another.	Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process your data.	Data Security; Security Measures (Cloud Data Processing Addendum)

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
	Your privileged administrative accounts probably have access to large volumes of data. Constraining the permissions of individual users to those absolutely necessary can help to limit the damage caused by malicious users, compromised credentials or compromised devices. Role-based access control provides a mechanism to achieve this and is likely to be a particularly important capability for users managing larger deployments. Exposing management interfaces to less accessible networks (e.g. community rather than public networks) makes it more difficult for attackers to reach and attack them, as they would first need to gain access to one of these networks.	For Google employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources, such as employee email and Google's internal employee portal. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Approvals are managed by workflow tools that maintain audit records of all changes. For customers, Google offers our tools and services such as Cloud Identity and Access Management which helps to prevent unauthorized access by controlling access rights and roles for Google Cloud Platform resources.	
44	**Principle 10: Identity and Authentication**		
45	All access to service interfaces should be constrained to authenticated and authorised individuals. Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service. Importantly, authentication should occur over secure channels. Email, HTTP or telephone are vulnerable to interception and social engineering attacks.	Refer to Row 41 and Row 43 for more information on authentication and access management.	N/A
46	**Principle 11: External Interface Protection**		
47	All external or less trusted interfaces of the service should be identified and appropriately defended. If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be more significant. You can use different models to connect to cloud services which expose your enterprise systems to varying levels of risk.	This is a customer consideration. Google provides our customers with the tools to monitor their workloads and perform their own assessments. For example: ● Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). ● Cloud Logging is a fully managed service that performs at scale and can ingest application and system log data, as well as custom log data from GKE environments, VMs, and Google Cloud services. Cloud Logging allows you to	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
		analyze selected logs and accelerate application troubleshooting. - Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Collect metrics, events, and metadata from Google Cloud services, hosted uptime probes, application instrumentation, and a variety of common application components; visualize them on charts and dashboards; and manage alerts.	
48	**Principle 12: Secure Service Administration**		
49	Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. The design, implementation and management of administration systems should follow enterprise good practice, whilst recognising their high value to attackers.	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding access control and privilege management. Refer to Row 41 and Row 43 for more information on privileged access management.	Data Security (Cloud Data Processing Addendum)
50	**Principle 13: Audit Information For Users**		
51	You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.	Google recognizes that you need visibility into who did what, when, and where for all user activity on our service. Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. In particular, Cloud Audit Logs help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events. Additionally, you can monitor and control the limited actions performed by Google personnel on your data using these tools: - Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location). - Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.	N/A

#	Framework reference	Google Cloud commentary	Google Cloud Services Contract reference
52	**Principle 14: Secure Use of the Service**		
53	The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.	This is a shared responsibility between Google and the customer. Refer to Row 1 for more information around how Google secures our cloud services. For our customers, Google provides detailed information about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page Please review Google Infrastructure Security Design Overview | Solutions regarding defense-in-depth techniques deployed across our infrastructure.	N/A