### Control Group | CGO | CID | Control Specification | Consensus Assessment Questions | Consensus Assessment Answers | Notes
--- | --- | --- | --- | --- | --- | ---
**Application & Interface Security**
**Application Security**  
AIS-01  
AIS-01.1 Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.  
Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACSC Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?  
X  
Google uses a continuous build and release process informed by industry practices. The controls around code release are included in the scope of our 3rd party attestations.  
**AIS-01.2**  
Do you use an automated source code analysis tool to detect security defects in code prior to production?  
X  
Google follows a structured code development and release process that includes considerations for security defects. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.  
**AIS-01.3**  
Do you use manual source-code analysis to detect security defects in code prior to production?  
X  
Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.  
**AIS-01.4**  
Do you verify that all of your software supplier adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?  
X  
Google does not rely on software suppliers for critical services provided to customers. All critical products are developed by Google and follow a mature software development process.  
**AIS-01.5**  
(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?  
X  
Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.  
**Application & Interface Security**
**Customer Access Requirements**  
AIS-02  
AIS-02.1 Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.  
Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?  
X  
Customers must agree to Google's Terms of Service and Acceptable Use Policy prior to using Google Cloud. Please see: https://cloud.google.com/terms/ for current terms relating to Google Cloud Platform and G Suite products.  
**AIS-02.2**  
Are all requirements and trust levels for customers' access defined and documented?  
X  
The customer must identify the appropriate trust levels for access to Google Cloud and set sharing permissions accordingly. Customers are responsible for managing these types of features in their applications in Google's cloud environment.  
**Application & Interface Security**
**Data Integrity**  
AIS-03  
AIS-03.1 Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.  
Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?  
X  
Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture satisfies industry standards such as PCI-DSS, NIST 800-53, NIST Trust Services Criteria (SOC2), and ISO 27001 security objectives.  
**AIS-03.2**  
Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.  
X  
Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture satisfies industry standards such as PCI-DSS, NIST 800-53, NIST Trust Services Criteria (SOC2), and ISO 27001 security objectives.  
**Application & Interface Security**
**Data Security / Integrity**  
AIS-04  
AIS-04.1 Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and businesses functions to prevent improper disclosure, alteration, or destruction.  
Your Data Security Architecture designed using an industry standard (e.g., CSA, MISTRA/SAFEC, CSAC Trust Cloud Architectural Standard, FedRAMP, CAFIT, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?  
X  
The intent of this control does not apply to Google Cloud Platform. However, Google conducts integrity checks on data written to its storage systems to ensure availability and replication.  
**AIS-04.2**  
Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.  
Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SOA/CYBERX, GRC XML, SACA Cloud Computing Measurement Audit/Assurance Program, etc.)?  
X  
Google provides audits assertions using industry accepted formats. For more details please refer to: https://cloud.google.com/security/compliance  
**Audit Assurance & Compliance**
**Audit Planning**  
AAC-01  
AAC-01.1 Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.  
Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SOA/CYBERX, GRC XML, SACA Cloud Computing Measurement Audit/Assurance Program, etc.)?  
X  
Google provides audits assertions using industry accepted formats. For more details please refer to: https://cloud.google.com/security/compliance  
**Audit Assurance & Compliance**
**Independent Audits**  
AAC-02  
AAC-02.1 Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.  
Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?  
X  
Google makes its SOC2/ISO 27001 and similar third-party audit or certification reports available to customers.  
**AAC-02.2**  
Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?  
X  
Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the security and security of Google's network infrastructure.  
**AAC-02.3**  
Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?  
X  
Google conducts rigorous internal continuous testing of their application surface through various types of penetration test exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers.
Google maintains an internal audit program consistent with industry best practices and regulatory requirements. Google undergoes several independent third party audits to test for data safety, privacy, and security, as noted below:

- SOC 1 / 2 / 3 (SSAE 18 - Formerly SSAE 16/SAS 70)
- ISO 27001
- ISO 27017 / 27018
- PCI-DSS
- HIPAA

For a full list of available certificates and compliance materials, please refer to: https://cloud.google.com/security/compliance

Google makes its SOC 2/S report and ISO 27001, 27017, and 27018 certificate available to customers. For a list of available certificates and compliance materials, please refer to: https://cloud.google.com/security/compliance

Google makes its SOC 2/S report and ISO 27001, 27017, and 27018 certificate available to customers. For a list of available certificates and compliance materials, please refer to: https://cloud.google.com/security/compliance

| Audit Assurance & Compliance Information System Regulatory Mapping | AAC-02.6 | Are the results of the penetration tests available to tenants at their request? | X | Google's Security Policy prohibits sharing this information but customers may conduct their own testing of our products and services. |
| Business Continuity Management & Operational Resilience Business Continuity Planning | AAC-02.7 | Are the results of internal and external audits available to tenants at their request? | X | Google makes its SOC 2/S report and ISO 27001, 27017, and 27018 certificate available to customers. For a list of available certificates and compliance materials, please refer to: https://cloud.google.com/security/compliance |
| | AAC-02.8 | Do you have an internal audit program that allows for cross-functional audit of assessments? | X | Google maintains an internal audit program consistent with industry best practices and regulatory requirements. Google's corporate Internal Audit team covers multiple disciplines and operational aspects of Google, including cross-functional audit of assessments. |
| | AAC-03.1 | Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected. | X | Customer data is logically segregated by domain to allow data to be produced for a single tenant. However, it is the responsibility of the customer to deal with legal requests. Google will provide customers with assistance with these requests, if necessary. |
| | AAC-03.2 | Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data? | X | Google has built multiple redundancies in its systems to prevent permanent data loss. Data durability assurances are built into the service specific terms as part of the terms of service. |
| | AAC-03.3 | Do you have the capability to recover data for a specific customer in the case of a failure or data loss? | X | Customers can choose data location in the US and Europe when configuring some of their Google Cloud Platform services. If these selections are made around choice of data location, this is backed by the service specific terms within Google’s Terms of Service. |
| | AAC-03.4 | Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data? | X | Google continuously surveys its compliance landscape and adjusts its policies and practices as needed. It is the customer's responsibility to configure the services and to be in compliance with any requirements relevant to their operations or jurisdictions. |
| | SCR-01.1 | A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:  
  - Defined purpose and scope, aligned with relevant dependencies  
  - Accessible to and understood by those who will use them | X | Google operates a global network of data centers to reduce risks from geographical disruptions. The link below includes the locations of our data centers:  
  - G Suite: https://www.google.com/about/datacenters/inside/locations/  
  - Google Cloud Platform: https://cloud.google.com/about/locations/  
  - For customers using Google Cloud’s CDN, the following locations apply: https://cloud.google.com/cdn/docs/locations |
Google provides documentation to customers to develop failover mechanisms for their cloud services. Customers can export/import an entire VM (Virtual Machine) image in the form of a .tar archive. These files can be backed up and stored in off-site locations or taken to a new cloud provider if needed. If using virtual infrastructure, does your cloud provider allow you to replicate those images in their own off-site storage location? Are business continuity plans subject to test at planned intervals? Google performs annual testing of its business continuity plans to simulate disaster scenarios that model catastrophic events that may disrupt Google operations.

Business Continuity Management & Operational Resilience

Do you provide tenants with infrastructure failover capability to other providers? Google provides documentation to customers to develop failover mechanisms for their environment. Failover to other providers is a customer responsibility.

Customers can choose data location in the US and Europe when configuring some of their Google Cloud Platform services. These selections are made around choice of data location, this is backed by the service specific terms within Google’s Terms of Service.

Business Continuity Management & Operational Resilience

Are business continuity plans subject to test at planned intervals? Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes? Business continuity plans involve impacted customers (tenants) and other business relationships that represent critical intra-supply chain business process dependencies.

Business Continuity Management & Operational Resilience

Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks to the extent possible. Google carefully selects the locations of its datacenters to avoid exposure to high-impact environmental risks to the extent possible.

Business Continuity Management & Operational Resilience

Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel? Information system documents (e.g., administrator and user guides, architecture diagrams, etc.) shall be made available to authorized personnel to ensure the following: Effectively using the system’s security features, Configuring, installing, and operating the information system, and Designing and Implementing system security controls.

Business Continuity Management & Operational Resilience

Are physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied? Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.

Business Continuity Management & Operational Resilience

Do you provide tenants with documentation showing the transport route of their data between your systems? Customers can choose data location in the US and Europe when configuring some of their Google Cloud Platform services. If these selections are made around choice of data location, this is backed by the service specific terms within Google’s Terms of Service.

Business Continuity Management & Operational Resilience

Can tenants define how their data is transported and through which legal jurisdictions? Can tenants define how their data is transported and through which legal jurisdictions? Engineering teams maintain procedures to facilitate the rapid reconstitution of services.

Business Continuity Management & Operational Resilience

Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: Effectively using the system’s security features, Configuring, installing, and operating the information system, and Designing and Implementing system security controls.

Business Continuity Management & Operational Resilience

Are your data centers located in places that have a high probability/occurrence of high-impact environmental risks to the extent possible. Google carefully selects the locations of its datacenters to avoid exposure to high-impact environmental risks to the extent possible.

Business Continuity Management & Operational Resilience

Customers can choose data location in the US and Europe when configuring some of their Google Cloud Platform services. If these selections are made around choice of data location, this is backed by the service specific terms within Google’s Terms of Service.
GCE VM image exports/imports are OS/software independent. Do you have a documented procedure for
security and redundancy measures and
implemented to protect equipment from utility
service outages (e.g., power failures, network
disruptions, etc.)?

Google has implemented redundancies and safeguards in its datacenters to minimize the impact
of service outages.

There shall be a defined and documented method for determining the
impact of any disruption to the organization (cloud provider, cloud
consumer) that must incorporate the following: • Identify critical products and services
• Identify all dependencies, including processes, applications, business
partners, and third party service providers • Understand threats to critical products and services
• Determine impacts resulting from planned or unplanned disruptions
and how these vary over time

Google maintains a dashboard for service availability information and service issues:

https://status.cloud.google.com/

https://www.google.com/appsstatus

Service Level Agreements may be found at: https://cloud.google.com/terms

Are security mechanisms and redundancies
independent restore and recovery capabilities?

Yes

Does your cloud solution include software/provider
independent restore and recovery capabilities?

X

Does your cloud solution include software/provider
independent restore and recovery capabilities?

No

Does your cloud solution include software/provider
independent restore and recovery capabilities?

Yes

Are security mechanisms and redundancies
implemented to protect equipment from utility
service outages (e.g., power failures, network
disruptions, etc.)?

Yes

Are you testing your backup or redundancy mechanisms
and how these vary over time?

Yes

Do you provide tenants with ongoing visibility and
reporting of your operational Service Level
Agreement (SLA) performance?

Yes

Do you provide tenants with ongoing visibility and
reporting of your operational Service Level
Agreement (SLA) performance?

No

Are you testing your backup or redundancy mechanisms
and how these vary over time?

No

Do you have a documented procedure for
responding to requests for tenant data from
governments or third parties?

Yes

Customers are responsible for managing their data retention policies. Customers may leverage
the features of our storage services. Please see product documentation for specifics:

https://cloud.google.com/docs/long-term-data-retention

https://cloud.google.com/storage/docs/bucket-lock

G Suite customers may purchase Google Vault to define organizational retention periods:

https://gsuite.google.com/learning-center/

For G Suite related installation, configuration and use of products/services/features, please refer to:

https://cloud.google.com/docs/gsuite

For G Suite related installation, configuration and use of products/services/features, please refer to:

https://gsuite.google.com/learning-center/
| Change Control & Configuration Management | CCC-02.1 | External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes). |
| Change Control & Configuration Management | CCC-02.2 | Do you have controls in place to detect source code security defects for any outsourced software development activities? |
| Change Control & Configuration Management | CCC-03.1 | Organization shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services. |
| Change Control & Configuration Management | CCC-03.2 | Do you provide tenants with documentation that describes your quality assurance process? |
| Change Control & Configuration Management | CCC-03.3 | Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? |
| Change Control & Configuration Management | CCC-03.4 | Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? |
| Change Control & Configuration Management | CCC-04.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. |
| Change Control & Configuration Management | CCC-05.1 | Policies and procedures shall be established for managing the risks associated with applying changes to: |
| Change Control & Configuration Management | CCC-06.1 | Do you have controls in place to ensure that standards of quality are being met for all software development? |
| Change Control & Configuration Management | CCC-07.1 | Do you have controls in place to detect source code security defects for any outsourced software development activities? |
| Change Control & Configuration Management | CCC-08.1 | Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? |
| Change Control & Configuration Management | CCC-09.1 | Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? |
| Data Security & Information Lifecycle Management Classification | DSI-01.1 | Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to organization. |
| Data Security & Information Lifecycle Management Classification | DSI-01.2 | Do you have a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)? |
| Data Security & Information Lifecycle Management Classification | DSI-02.1 | Do you have a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)? |
| Data Security & Information Lifecycle Management Classification | DSI-02.2 | Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)? |
| Data Security & Information Lifecycle Management Classification | DSI-03.1 | Do you have controls in place to ensure that standards of quality are being met for all software development? |
| Data Security & Information Lifecycle Management Classification | DSI-03.2 | Do you have controls in place to detect source code security defects for any outsourced software development activities? |
| Data Security & Information Lifecycle Management Classification | DSI-04.1 | Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? |
| Data Security & Information Lifecycle Management Classification | DSI-04.2 | Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? |
| Data Security & Information Lifecycle Management Classification | DSI-05.1 | Policies and procedures shall be established for managing the risks associated with applying changes to: |
| Data Security & Information Lifecycle Management Classification | DSI-05.2 | Do you have controls in place to ensure that standards of quality are being met for all software development? |
| Data Security & Information Lifecycle Management Classification | DSI-06.1 | Do you have controls in place to detect source code security defects for any outsourced software development activities? |
| Data Security & Information Lifecycle Management Classification | DSI-07.1 | Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? |
| Data Security & Information Lifecycle Management Classification | DSI-07.2 | Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? |
| Data Security & Information Lifecycle Management Classification | DSI-08.1 | Policies and procedures shall be established for managing the risks associated with applying changes to: |
| Data Security & Information Lifecycle Management Classification | DSI-09.1 | Do you have controls in place to ensure that standards of quality are being met for all software development? |
| Data Security & Information Lifecycle Management Classification | DSI-09.2 | Do you have controls in place to detect source code security defects for any outsourced software development activities? |
| DSI-01.3 | Do you have a capability to use system geographic location as an authentication factor? | X | Google allows domain administrators to configure alerts for potential suspicious logins. Geographic location is one factor that could indicate a suspicious login. |
| DSI-01.4 | Can you provide the physical location/geography of storage of a tenant’s data upon request? | X | Google may store customer data in the following locations: |
| DSI-01.5 | Can you provide the physical location/geography of storage of a tenant’s data in advance? | X | Google may store customer data in the following locations: |
| DSI-01.6 | Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)? | X | Customers can apply their own data-labeling standard to information stored in Google Cloud. |
| DSI-01.7 | Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation? | X | Customers may select where certain Customer Data will be stored ("Data Location Selection"), and Google will store it in accordance with the Service Specific Terms. |

**Data Security & Information Lifecycle Management**

**Data Inventory / Flows**

| DSI-02 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanent or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services. | X | Network flow policies are enforced through switch and router based ACLs. Network traffic dashboard and automated inventory tools provide real-time information on traffic flow enforcement. |
| DSI-02.1 | Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data. | | Google supports the use of open encryption methodologies. Google forces TLS for all authentication traffic. Customer data is encrypted when on Google’s internal networks, in transport and at rest. |
| DSI-02.2 | Can you ensure that data does not migrate beyond a defined geographical residency? | X | Google uses encryption when customer data traverses public networks. Encryption may be open-source based or proprietary. |

**Data Security & Information Lifecycle Management**

**E-commerce Transactions**

| DSI-03 | Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. | X | Google maintains policies and procedures on data access and labeling. |
| DSI-03.1 | Do you provide open encryption methodologies (3.4 ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)? | X | Google maintains policies and procedures on data access and labeling. |
| DSI-03.2 | Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., internet-based replication of data from one environment to another)? | X | Google maintains policies and procedures on data access and labeling. |

**Data Security & Information Lifecycle Management**

**Handling / Labeling / Security Policy**

| DSI-04 | Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. | X | This control is not applicable to Google Cloud. |
| DSI-04.1 | Are policies and procedures established for labeling, handling and the security of data and objects that contain data? | X | Google maintains policies and procedures on data access and labeling. |
| DSI-04.2 | Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data? | X | Google maintains policies and procedures on data access and labeling. |

**Data Security & Information Lifecycle Management**

**Nonproduction Data**

| DSI-05 | Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements. | | Google has established procedures and technical controls to help ensure production data remains in the secure boundary of the production network. |
| DSI-05.1 | Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments? | X | Google’s terms of service address data ownership and its internal data security policies govern data stewardship. |

**Data Security & Information Lifecycle Management**

**Ownership / Stewardship**

<p>| DSI-06 | All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated. | X | Google’s terms of service address data ownership and its internal data security policies govern data stewardship. |</p>
<table>
<thead>
<tr>
<th>Data Security &amp; Information Lifecycle Management</th>
<th>Secure Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy:</strong></td>
<td><strong>Datacenter Security Policy</strong></td>
</tr>
<tr>
<td><strong>SECURITY PROCEDURES:</strong></td>
<td><strong>SECURITY PROCEDURES:</strong></td>
</tr>
<tr>
<td><strong>DCS-01:</strong></td>
<td><strong>DCS-01.1:</strong> Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities. Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?</td>
</tr>
<tr>
<td><strong>DCS-02:</strong></td>
<td><strong>DCS-02.1:</strong> Physical security perimeters (e.g., fences, walls, barriers, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems. Are physical security perimeters (e.g., fences, walls, barriers, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?</td>
</tr>
<tr>
<td><strong>DCS-03:</strong></td>
<td><strong>DCS-03.1:</strong> Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location. Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?</td>
</tr>
<tr>
<td><strong>DCS-04:</strong></td>
<td><strong>DCS-04.1:</strong> Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises. Do you provide tenants with documentation that describe how we operate a global network with replication, failover, and offsite backups?</td>
</tr>
<tr>
<td><strong>DCS-05:</strong></td>
<td><strong>DCS-05.1:</strong> Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization’s premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse or deployment or securely stored until it can be destroyed. Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?</td>
</tr>
<tr>
<td><strong>DCS-06:</strong></td>
<td><strong>DCS-06.1:</strong> Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?</td>
</tr>
<tr>
<td><strong>DCS-06.2:</strong></td>
<td><strong>DCS-06.2:</strong> Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?</td>
</tr>
</tbody>
</table>
Datacenter Security

**Secure Area Authorization**

DCS-07

**DCS-07.1**

Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.

Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of based on legal and jurisdictional considerations? X

Customers can choose data location when they initiate project set up. This is covered by our service specific terms:

https://cloud.google.com/terms/service-terms

Google Cloud Platform customers may select specific regions to place data, based on product availability.

G Suite customers benefit from a globally distributed environment. G Suite tenants are made aware of all data center locations where G Suite data may reside.

**Datacenter Security Unauthorized Persons Entry**

DCS-08

DCS-08.1

Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.

Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process? X

Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system 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 via digital video recorders 24 hours a day, 7 days a week.

**Datacenter Security User Access**

DCS-09

DCS-09.1

Physical access to information assets and functions by users and support personnel shall be restricted.

Do you restrict physical access to information assets and functions by users and support personnel? X

Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors, and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request (which is followed by proper approval process) electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor’s manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center manager for the specific data center and internal areas they wish to visit; (ii) sign in at on site security operations; (iii) reference an approved data center access record identifying the individual as approved.

**Encryption & Key Management**

**Key Generation**

EMM-01

EMM-01.1

Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.

Do you have key management policies binding keys to identifiable owners? X

Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.

EMM-02

EMM-02.1

Policies and procedures shall be established for the management of cryptographic keys in the service’s cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.

Do you have a capability to allow creation of unique encryption keys per tenant? X

Google provides capabilities to encrypt data by tenant for a subset of products:

https://cloud.google.com/security/encryption-at-rest/

EMM-02.2

Do you have a capability to manage encryption keys on behalf of tenants? X

Google has capabilities to manage encryption keys on behalf of tenants.

EMM-02.3

Do you maintain key management procedures? X

Google maintains documentation on its key management process.

EMM-02.4

Do you have documented ownership for each stage of the lifecycle of encryption keys? X

Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.

EMM-02.5

Do you utilize any third party/open source/proprietary frameworks to manage encryption keys? X

Google uses a combination of open source and proprietary code to develop its encryption solutions.

**Encryption & Key Management Encryption**

EMM-03

EMM-03.1

Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.

Do you encrypt tenant data at rest (on disk/storage) within your environment? X

Google maintains encryption at rest for customer data.

EMM-03.2

Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances? X

Google employs several security measures to help ensure the authenticity, integrity, and privacy of data in transit.

Encryption In Transit Whitepaper:


G Suite Encryption Whitepaper:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?</td>
<td>X</td>
<td>Google maintains documentation for the use of its internal proprietary key management service.</td>
</tr>
<tr>
<td>Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?</td>
<td>X</td>
<td>For details refer to: <a href="https://cloud.google.com/storage/docs/encryption/customer-managed-keys">https://cloud.google.com/storage/docs/encryption/customer-managed-keys</a></td>
</tr>
<tr>
<td>Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?</td>
<td>X</td>
<td>Google uses a combination of open source and proprietary encryption formats and algorithms validated by Google security engineers.</td>
</tr>
<tr>
<td>Are your encryption keys maintained by the cloud consumer or a trusted key management provider?</td>
<td>X</td>
<td>Google maintains its own encryption keys.</td>
</tr>
<tr>
<td>Do you store encryption keys in the cloud?</td>
<td>X</td>
<td>Google stores its keys in its own production environment.</td>
</tr>
<tr>
<td>Do you have separate key management and key usage duties?</td>
<td>Google’s key management operates as a service for engineering teams to use in their application code.</td>
<td></td>
</tr>
</tbody>
</table>

### Governance and Risk Management
**Baseline Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you have documented information security baselines for every component of your infrastructure?</td>
<td>X</td>
<td>Google maintains security configurations for its machines and networking devices. The configurations are maintained and serve as master copies for comparison against production instances. Deviations are identified and corrected.</td>
</tr>
<tr>
<td>Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?</td>
<td>X</td>
<td>Google has automated mechanisms to detect deviations from the desired security configuration of its infrastructure.</td>
</tr>
<tr>
<td>Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?</td>
<td>X</td>
<td>Google allows customers to use their own virtual image to use in Google Cloud Platform. <a href="https://cloud.google.com/compute/docs/tutorials/building-images">https://cloud.google.com/compute/docs/tutorials/building-images</a></td>
</tr>
</tbody>
</table>

**Risk Assessments**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?</td>
<td>X</td>
<td>Google Cloud Platform provides the ability to log and monitor security and system health. <a href="https://cloud.google.com/security-command-center/">https://cloud.google.com/security-command-center/</a></td>
</tr>
<tr>
<td>Do you conduct risk assessments associated with data governance requirements at least once a year?</td>
<td>X</td>
<td>Google performs risk assessments as required to support its ISMS.</td>
</tr>
</tbody>
</table>

**Management Oversight**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are your technical, business, and executive managers responsible for ensuring direct reports complete all required trainings and attestations? Sanctions are in place for Googlers who do not complete required training within the required time period.</td>
<td>X</td>
<td>Management is responsible for ensuring direct reports complete all required trainings and attestations. Sanctions are in place for Googlers who do not complete required training within the required time period.</td>
</tr>
</tbody>
</table>

**Management Program**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business:</td>
<td>X</td>
<td>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 27001 certification.</td>
</tr>
<tr>
<td>Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?</td>
<td>X</td>
<td>Google provides customer-managed encryption keys where tenants can generate and manage their own encryption keys using Cloud Key Management Service for a specific set of services.</td>
</tr>
<tr>
<td>Do you review your Information Security Management Program (ISMP) least once a year?</td>
<td>X</td>
<td>Google reviews its ISMS documentation annually as part of its required due diligence.</td>
</tr>
</tbody>
</table>
Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization’s business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.

Do you ensure your providers adhere to your information security and privacy policies?

X

Google maintains a robust vendor management program. Vendors who work with Google are required to comply with all relevant information security and privacy policies. In addition, Google has open-sourced its vendor management questionnaires for use by the community:

https://opensource.googleblog.com/2016/03/scalable-vendor-security-reviews.html

Information security policies and procedures shall be established and align with industry standards (ISO-27001, ISO-22307, COBIT, etc.)?

X

Google’s security and privacy policies align with ISO 27001.

Do you have agreements to ensure your providers adhere to your information security and privacy policies?

X

Google agrees contractually with providers on adherence to Google’s security and privacy policies and has a vendor audit program to determine compliance.

Are you made aware of what actions could be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures?

X

Google maintains a personnel policy that includes disciplinary procedures.

Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.

Do you perform, at minimum, annual reviews to assess your security programs and policies?

X

Google makes its internal policies available to all personnel. Communication of policies occurs via required training, and through ongoing e-mail and internal communication. Employees must review and confirm understanding of key security and privacy policies (including what actions are taken if an employee is in violation of said policy) at least annually, and records of certification are retained to ensure compliance.

Google's code of conduct is available publicly at our investor website.

https://cloud.google.com/security/compliance/

A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.

Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?

X

Google maintains a personnel policy that includes disciplinary procedures.

The organization’s business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continued alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.

Do you notify your tenants when you make material changes to your information security and/or privacy policies?

X

Google notifies tenants of material changes to contractually committed terms. Google does not notify tenants of changes to internal policies.

Do you perform, at minimum, annual reviews to your privacy and security policies?

X

Google reviews its security and privacy policies at least annually. Google’s cross functional security policy team meets periodically throughout the year to address emerging issues and risk and issue new or amend existing policies or guidelines, as needed.

Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).

Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?

X

Google’s risk assessments are conducted annually and are aligned with the enterprise risk framework. The risk assessment uses both qualitative and quantitative methods to determine likelihood and impact of events.

Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.

Do you have a documented, organization-wide program in place to manage risk?

X

Google has documented its risk management procedures as part of its ISMS that underlies our ISO 27001 certification.

Do you make available documentation of your organization-wide risk management program?

X

Google has documented its risk management procedures as part of its ISMS that underlies our ISO 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs.

Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?

X

Google's security incident response process includes involvement of our privacy team. Customers are notified when an event impacts their data.
| HRS-01.2 | Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk. | Is your Privacy Policy aligned with industry standards? | X | Google's privacy policy is informed by industry standards and tailored to Google's unique operational environment. |
| HRS-02.3 | Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk. | Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. |
| HRS-03.1 | Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full- or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets. | Do you specifically train your employees regarding their specific role and the information security controls they must fulfill? | X | Google provides role-specific privacy and security training. The training is administered online and completion is tracked. Privacy and security training are required annually. |
| HRS-04.1 | Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. | Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities))? | X | Google maintains a mobile device policy that details our requirements for mobile device use at Google. Customer data is not permitted on mobile devices. |
| HRS-04.2 | Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated. | Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities))? | X | Google maintains a mobile device policy that details our requirements for mobile device use at Google. Customer data is not permitted on mobile devices. |
| HRS-05.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring). | Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationalization, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data? | X | Google provides Google-specific security training. The training is administered online and completion is tracked. Completion is required annually. |
Human Resources
User Responsibility

RIS-09.2 Are users made aware of their responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations?

X Customers are responsible for ensuring proper education and identifying legal responsibilities of their staff as it relates to customer applications and data. Google personnel are trained on the Data Security policy including procedures for handling customer data.

RIS-10

All personnel shall be made aware of their roles and responsibilities for:

RIS-10.1.1 Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.

RIS-10.2 Maintaining a safe and secure working environment

RIS-10.3 Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?

X Google maintains a security awareness program for its personnel. Customers are responsible for training their users.

RIS-11 Policies and procedures shall be established to require that unauthorized workplaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.

X Google maintains a Data Security Policy that governs conflict of interests.

RIS-11.2 Do you monitor and log privileged access to your data management policies and procedures, address tenant and service level conflicts of interest?

X Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access.

RIS-11.3 Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the virtual machine?

X Google's production environment is segregated from the corporate environment.

RIS-12 Do you restrict and log access to your source code, and assure it is restricted to authorized personnel only?

X Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools.

RIS-13 Do you provide multi-failure disaster recovery capability?

X Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy and detect unauthorized access.

Identity & Access Management

Audit Tools Access

IAM-01 Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.

X Google maintains automated log collection and analysis tools. Multi-factor authentication is required for any connections to our production environment.

IAM-01.1 Do you restrict, log and monitor access to your information security management systems? (e.g., firewalls, vulnerability scanners, network sniffers, APIs, etc.)

X Google maintains automated log collection and analysis tools. Multi-factor authentication is required for any connections to our production environment.

IAM-02 How does the organization monitor and log activity that may be a violation of its policies?

X Google's code of conduct is available publically at our investor website: https://investor.google.com/corporate/code-of-conduct.html.

IAM-02.1 Google makes its personnel policy available to all personnel and reminds employees as part of training and ongoing email communication action that may be a violation of its policies. Google's code of conduct is available publically at our investor website: https://investor.google.com/corporate/code-of-conduct.html.

X Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment.

IAM-02.2 Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?

X Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment.

IAM-03 User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.

X Google logs all changes in user permissions with the date and time of such changes.

IAM-03.1 Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?

X Google logs all changes in user permissions with the date and time of such changes.

IAM-04 Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.

X Google's production environment is segregated from the corporate environment.

IAM-04.1 Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?

X Google maintains a central identity and authorization management system.

IAM-04.2 Do you manage and store the identity of all personnel who have network access, including their level of access?

X Google maintains a central identity and authorization management system.

Identity & Access Management
Policies and Procedures

IAM-05 Are users made aware of their responsibilities for access to your application, program or object source code, and assure it is restricted to authorized personnel only?

X Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper

IAM-05.1 Do you provide tenants with documentation on how to maintain segregation of duties within your cloud service offering?

X Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

IAM-06 Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.

X Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools.

IAM-06.1 Are there controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?

X Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools.

IAM-06.2 Are there controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?

X Google automatically replicates to and serves data from multiple data centers to provide seamless access to end-users should a datacenter not be available.

Identity & Access Management
Source Code Access Restriction

IAM-07.1 The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to

X Google has designed redundancies in its system to help prevent service interruptions in the event of failure within Google or a provider-operated infrastructure.

IAM-07.2 Do you monitor service continuity with upstream providers in the event of provider failure?

X Google has designed redundancies in its system to help prevent service interruptions in the event of failure within Google or a provider-operated infrastructure.

IAM-07.3 Do you have more than one provider for each service you depend on?

X Google maintains redundancy for critical services such as telecommunication links.

Identity & Access Management
Diagnostic/Configuration Parts Access

IAM-08 Diagnostic / Configuration Ports

IAM-08.1 Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.

X Google's production environment is segregated from the corporate environment.

IAM-08.2 Do you use dedicated secure networks to provide management access to your cloud service infrastructure?

X Google's production environment is segregated from the corporate environment.

IAM-08.3 Do you use dedicated secure networks to provide management access to your cloud service infrastructure?

X Google's production environment is segregated from the corporate environment.

IAM-08.4 Do you manage and store the identity of all personnel who have network access, including their level of access?

X Google maintains a central identity and authorization management system.

IAM-08.5 Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?

X Google maintains a central identity and authorization management system.

Identity & Access Management
Segregation of Duties

IAM-09 User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per definition of segregation of duties to address business risks associated with a user-role conflict of interest.

X Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper

IAM-09.1 Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?

X Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

IAM-09.2 Are controls in place in your software infrastructure to detect and correct deviations from its security baselines and collects and secures audit records.

X Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

IAM-09.3 Are controls in place in your software infrastructure to detect and correct deviations from its security baselines and collects and secures audit records.

X Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

Identity & Access Management
User Access Policy

X Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

IAM-02.3 Do you provide multi-failure disaster recovery process that include account locking and revocation of certificates and role assignment?

X Google's production environment is segregated from the corporate environment.

IAM-02.4 Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?

X Google logs all changes in user permissions with the date and time of such changes.

IAM-03.2 Do you use dedicated secure networks to provide management access to your cloud service infrastructure?

X Google's production environment is segregated from the corporate environment.

IAM-03.3 Do you use dedicated secure networks to provide management access to your cloud service infrastructure?

X Google's production environment is segregated from the corporate environment.

IAM-04.3 Do you manage and store the identity of all personnel who have network access, including their level of access?

X Google maintains a central identity and authorization management system.

IAM-04.4 Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?

X Google maintains a central identity and authorization management system.

IAM-05.2 Do you provide tenants with documentation on how to maintain segregation of duties within your cloud service offering?

X Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper

IAM-05.3 Are there controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?

X Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

IAM-05.4 Are there controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?

X Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
<table>
<thead>
<tr>
<th>Title</th>
<th>Body</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity &amp; Access Management</strong>&lt;br&gt;&lt;br&gt;<strong>User Access Restriction / Authorization</strong>&lt;br&gt;&lt;br&gt;<strong>IAM-07.4</strong></td>
<td>Do you provide access to operational redundancy and continuity summaries, including the services you depend on? X</td>
</tr>
<tr>
<td><strong>IAM-07.5</strong></td>
<td>Do you provide the tenant the ability to declare a disaster? X</td>
</tr>
<tr>
<td><strong>IAM-07.6</strong></td>
<td>Do you provided a tenant-triggered failover option? X</td>
</tr>
<tr>
<td><strong>IAM-07.7</strong></td>
<td>Do you share your business continuity and redundancy plans with your tenants? X</td>
</tr>
<tr>
<td><strong>IAM-08.1</strong></td>
<td>Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.</td>
</tr>
<tr>
<td><strong>IAM-08.2</strong></td>
<td>Do you have a method of aligning provider and tenant data classification methodologies for access control purposes? X Not Applicable</td>
</tr>
<tr>
<td><strong>Identity &amp; Access Management</strong>&lt;br&gt;&lt;br&gt;<strong>User Access Authorization</strong>&lt;br&gt;&lt;br&gt;<strong>IAM-09.1</strong></td>
<td>Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components? X Customers are responsible for configuring the access by their users to the service. For Google personnel, authorization is required prior to access being granted.</td>
</tr>
<tr>
<td><strong>IAM-09.2</strong></td>
<td>Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components? X Customers are responsible for configuring the access by their users to the service. For Google personnel, authorization is required prior to access being granted.</td>
</tr>
<tr>
<td><strong>Identity &amp; Access Management</strong>&lt;br&gt;&lt;br&gt;<strong>User Access Reviews</strong>&lt;br&gt;&lt;br&gt;<strong>IAM-10.1</strong></td>
<td>User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization’s business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rules of least privilege based on function. For identified access violations, remediation must follow established user access policies and procedures. Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)? X Google requires access reviews at least bi-annually for critical access groups.</td>
</tr>
<tr>
<td><strong>IAM-10.2</strong></td>
<td>If users are found to have inappropriate entitlements, are all remediation and certification actions recorded? X Google logs all changes in user permissions. Google revokes access when no longer required.</td>
</tr>
<tr>
<td><strong>IAM-10.3</strong></td>
<td>Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data? X Google notifies customers of security incidents that impact their data and will work with the customer in good faith to address any known breach of Google’s security obligations.</td>
</tr>
<tr>
<td><strong>Identity &amp; Access Management</strong>&lt;br&gt;&lt;br&gt;<strong>User Access Revocation</strong>&lt;br&gt;&lt;br&gt;<strong>IAM-11.1</strong></td>
<td>Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control. Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties? X Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically reviews access lists and removes access that is no longer required. All account actions are recorded.</td>
</tr>
<tr>
<td><strong>IAM-11.2</strong></td>
<td>Any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization? X Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically reviews access lists and removes access that is no longer required. All account actions are recorded.</td>
</tr>
</tbody>
</table>
### Identity & Access Management - User ID Credentials

**IAM-12.1 Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:**

- Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)
- Account credential lifecycle management from instantiation through revocation
- Account credential and/or identity store minimization or re-use when feasible
- Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?</td>
<td>X</td>
</tr>
<tr>
<td>Do you use open standards to delegate authentication capabilities to your tenants?</td>
<td>X</td>
</tr>
<tr>
<td>Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?</td>
<td>X</td>
</tr>
<tr>
<td>Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?</td>
<td>X</td>
</tr>
<tr>
<td>Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?</td>
<td></td>
</tr>
<tr>
<td>Do you provide tenants with strong (multi-factor) authentication options (digital certs, tokens, biometrics, etc.) for user access?</td>
<td>X</td>
</tr>
<tr>
<td>Do you allow tenants to use third-party identity assurance services?</td>
<td>X</td>
</tr>
<tr>
<td>Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?</td>
<td>X</td>
</tr>
<tr>
<td>Do you allow tenants/customers to define password and account lockout policies for their accounts?</td>
<td>X</td>
</tr>
<tr>
<td>Do you support the ability to force password changes upon first login?</td>
<td>X</td>
</tr>
<tr>
<td>Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock?)</td>
<td>X</td>
</tr>
</tbody>
</table>

### Identity & Access Management - Utility Programs Access

**IAM-13.1 Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted:**

- Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored? | X | ACLs for production tools are appropriately scoped to perform job function. [Link](https://cloud.google.com/iam/identity) |
| Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)? | X | Google continuously monitors our cloud infrastructure. [Link](https://cloud.google.com/iam/identity) |
| Are attacks that target the virtual infrastructure prevented with technical controls? | X | The cloud platform infrastructure is appropriately hardened to minimize attack surface. [Link](https://cloud.google.com/iam/identity) |
### Infrastructure & Virtualization Security Audit Logging / Intrusion Detection

| VS-01.1 | Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. | X | | Google has implemented network and host based tools to detect and respond to potential security incidents. Google maintains automated log collection and analysis tools to support investigations. |

| VS-02.1 | Are file integrity (hash) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents? | X | | Google restricts physical and logical access to audit logs. |

| VS-03.1 | If physical and logical user access to audit logs restricted to authorized personnel? | X | | Google has mapped its security controls to the requirements of the AICPA Trust Services Criteria (SOC2), NIST 800-53, and ISO 27002. Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |

### Infrastructure & Virtualization Security Change Detection

| VS-01.1 | The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts). | X | | Google maintains an automated log collection and analysis tool to review and analyze log events. |

| VS-02.2 | Are audit logs centrally stored and retained? | X | | Google maintains an automated log collection and analysis tool to review and analyze log events. |

### Infrastructure & Virtualization Security Clock Synchronization

| VS-01.1 | A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstruction of activity timelines. | X | | | Google uses a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference. Google makes their NTP protocol public as well for use by customers. |

### Infrastructure & Virtualization Security Capacity / Resource Planning

| VS-01.1 | The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload. | X | | Google maintains an effective resource economy with internal SLAs between engineering teams that provide for capacity planning and provisioning decisions. |

| VS-03.2 | Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off, or running)? | X | | Cloud Security Command Center provides visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems. Please see https://cloud.google.com/security-command-center/docs/ for more information. In addition, Shielded VM’s enable live measurement, monitoring, and alerting for any changes of the full stack. |

| VS-04.3 | Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios? | X | | | Google maintans automated log collection and analysis tool to review and analyze log events. |

### Infrastructure & Virtualization Security Management - Vulnerability Management

| VS-01.1 | Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware). | X | | Google performs fuzz testing, penetration testing, and vulnerability scanning to detect, mitigate, and resolve security issues. |

### Infrastructure & Virtualization Security Network Security

| VS-01.1 | Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls. | X | | Google maintains network diagrams for internal purposes, but due to the dynamic and sensitive nature of the information, does not share it externally. |

| VS-02.3 | For your said offering, do you provide customers with guidance on how to create a layered security architecture equivalent using your virtualized solution? | X | | Google provides solution papers and reference docs for various architectures and intended solutions. |

| VS-03.3 | Do you regularly update network architecture diagrams that include data flows between security domains/zones? | X | | Google uses tools to detect and respond to potential security incidents. Google maintains automated log collection and analysis tools to support investigations. |

| VS-04.3 | Do you regularly review for appropriateness the allowed access/controls (e.g., firewall rules) between security domains/zones within the network? | X | | The security state of network devices is monitored continuously. |

| VS-05.4 | Are all firewall access control lists documented with business justification? | X | | Network ACLs are documented within configuration files with comments on purpose, as appropriate. |
Google builds its own machines and deploys custom operating system images that only permit the necessary ports, protocols, and services.

For its SaaS or PaaS offering, does Google provision tenants with separate environments for production and test purposes?

Customers can provision separate domains or organizations within a domain for testing purposes. Google provides solution papers and reference docs for development and test environments: https://cloud.google.com/solutions/devtest/

Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtualized servers?

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. Please see https://cloud.google.com/security/encryption-in-transit/ for more information.

Are系统和network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Is Google’s production network separate from other networks?

Google’s production network is separated from other networks.

Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?

Are operating systems hardened to provide only the necessary ports, protocols and services.

Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline operating build standard or template?

Do you logically and physically segregate production and non-production environments?

Google segregates its production environment from its corporate environment.

Are you logically and physically segregate production and non-production environments?

Google segregates its production environment from its corporate environment.

Do you logically and physically segregate production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?

Google segregates its production and corporate environments with appropriate network boundary controls.
<table>
<thead>
<tr>
<th>Interoperability &amp; Portability</th>
<th>APIs</th>
<th>Date Requested</th>
<th>Description</th>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interoperability &amp; Portability</td>
<td>APIs</td>
<td>PY-01</td>
<td>The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.</td>
<td>Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?</td>
<td>X</td>
</tr>
<tr>
<td>Interoperability &amp; Portability</td>
<td>Policy &amp; Legal</td>
<td>PY-03</td>
<td>Policies, procedures, and mutually-agreed upon provisions and terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.</td>
<td>Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?</td>
<td>X</td>
</tr>
<tr>
<td>Interoperability &amp; Portability</td>
<td>Standardized Network Protocols</td>
<td>PY-04</td>
<td>The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.</td>
<td>Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?</td>
<td>X</td>
</tr>
<tr>
<td>Interoperability &amp; Portability</td>
<td>Virtualization</td>
<td>PY-05</td>
<td>The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review.</td>
<td>Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?</td>
<td>X</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>Anti-Malware</td>
<td>MOS-01</td>
<td>Anti-malware awareness training, specific to mobile devices, shall be included in the provider’s information security awareness training.</td>
<td>Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?</td>
<td>X</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>Application Stores</td>
<td>MOS-02</td>
<td>A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.</td>
<td>Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?</td>
<td>X</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>Approved Applications</td>
<td>MOS-03</td>
<td>The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.</td>
<td>Do you have a policy enforcement capability (e.g., NACM) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?</td>
<td>X</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>Approved Software for BYOD</td>
<td>MOS-04</td>
<td>The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.</td>
<td>Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?</td>
<td>X</td>
</tr>
</tbody>
</table>
Mobile Security Awareness and Training

MOS-05
The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall provide and communicate the policy and requirements through the company’s security awareness and training program.

MOS-06
Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and acceptable usage and requirements for mobile devices?

X
Google provides security awareness training to all employees that includes references to our security policies, including our mobile device policies. Training also includes how to protect data when using mobile devices in public.

Mobile Security Cloud Based Services

MOS-06
All cloud-based services used by the company’s mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.

MOS-07
Do you have a documented list of pre-approved cloud-based services that are allowed to be used for use and storage of company business data via a mobile device?

X
Google only permits the storage of Google sensitive information in approved systems.

Mobile Security Compatibility

MOS-07
The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.

MOS-08
Do you have a documented application validation process for testing device, operating system and application compatibility issues?

X
Mobile operability is part of our standard software engineering development lifecycle.

Mobile Security Device Eligibility

MOS-08
The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.

MOS-09
Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?

X
Google maintains a mobile policy and provides detailed instructions to personnel that wish to provision access to Google services on their mobile device. The policy includes eligibility requirements and security policy requirements.

Mobile Security Device Inventory

MOS-09
An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for use (BYOD), will be included for each device in the inventory.

MOS-10
Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (OS system and patch levels, lost or decommissioned, device assigned)?

X
All devices must register through the Google Device Policy Manager unless browser-only access is used.

Mobile Security Device Management

MOS-10
A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.

MOS-11
Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?

X
Google’s Device Policy Manager enforces Google’s mobile policy except when access is solely to Apps services and through a browser.

Mobile Security Encryption

MOS-11
The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.

MOS-12
Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive through technology controls for all mobile devices?

X
Mobile devices with access to corporate resources other than Apps services require encryption.

Mobile Security Jailbreaking and Rooting

MOS-12
The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through protective andpreventive controls on the device or through a centralized device management system (e.g., mobile device management).

MOS-13
Do you have mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?

X
Google’s mobile policy does not permit jailbreaking or rooting on devices linked to a Google corporate account.

Mobile Security Legal

MOS-13
The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy clearly states the expectations over the loss of non-company data in the case of a wipe of the device is required.

MOS-14
Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?

X
Google’s mobile policy states that all security policies apply in a mobile environment.

Mobile Security Lockdown Screen

MOS-14
BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.

MOS-15
Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?

X
Google’s Device Policy Manager requires personnel to set an automatic lockout screen.

Mobile Security Operating Systems

MOS-15
Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company’s change management processes.

MOS-16
Do you manage all changes to mobile device operating systems, patch levels and applications via your company’s change management processes?

X
Google’s Device Policy Manager requires personnel to keep devices up to date with patches and requires a minimum OS level.

Mobile Security Passwords

MOS-16
Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.

MOS-17
Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?

X
Google’s Device Policy Manager enforces password policies.

Mobile Security Policy

MOS-17
The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).

MOS-18
Do you have a policy that requires BYOD users to perform backups of specified corporate data?

X
Data from Google services are synced from the cloud data store to the device.

MOS-12.1
Do you have a documented list of pre-approved applications that are allowed to be used for use and storage of company business data via a mobile device?

MOS-13.1
Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?

X
Google’s mobile policy does not permit jailbreaking or rooting on devices linked to a Google corporate account.

MOS-13.2
Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?

X
Google’s Device Policy Manager may not install on a device that does not conform to the required security specifictions. The Device Policy Manager is required in order to access corporate sources using mobile applications.

MOS-14.1
Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?

X
Google’s Device Policy Manager requires personnel to set an automatic lockout screen.

MOS-14.2
Do you have a documented application validation process for testing device, operating system and application compatibility issues?

X
Google’s mobile policy does not permit jailbreaking or rooting on devices linked to a Google corporate account.

MOS-15.1
Do you have a documented list of pre-approved applications that are allowed to be used for use and storage of company business data via a mobile device?

X
Google only permits the storage of Google sensitive information in approved systems.

MOS-16.1
Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?

X
Google’s Device Policy Manager enforces password policies.

MOS-16.2
Do you have a policy that requires BYOD users to perform backups of specified corporate data?

X
Data from Google services are synced from the cloud data store to the device.

MOS-16.3
Do you have a policy that requires BYOD users to perform backups of specified corporate data?

X
Data from Google services are synced from the cloud data store to the device.

MOS-17.1
Do you have a policy that requires BYOD users to perform backups of specified corporate data?

X
Data from Google services are synced from the cloud data store to the device.

MOS-17.2
Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?

X
Google’s mobile device policy does not permit the use of unapproved application stores.
| MOS-17.3 | All mobile devices permitted for use through the company BYOD program or a company-appointed mobile device shall allow for remote wipe by the company’s corporate IT or shall have all company-provided data wiped by the company’s corporate IT. | X | Google requires all mobile devices (including personally owned devices) to conform to corporate device management policies that apply restrictive controls to reduce the risk of malware-based attacks. |
| MOS-18.1 | Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices? | X | Google requires all mobile devices (including personally owned devices) to conform to device management policies, including remote wipe capabilities. |
| MOS-18.2 | Does your IT provide remote wipe or corporate data wipe for all company-appointed mobile devices? | X | Google requires remote wipe capabilities for all mobile devices managed by Google. |
| MOS-19.1 | Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely. | X | Google’s mobile policy requires the installation of all updates and sets minimum O/S requirements. |
| MOS-19.2 | Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? | X | Google’s mobile policy requires the installation of all updates and sets minimum O/S requirements. |
| MOS-20.1 | The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device. | X | Google’s mobile policy defines which corporate resources can be accessed with a mobile device and the level of protections associated with such access. |
| MOS-20.2 | Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device? | X | Google’s mobile policy defines which roles (profiles) can access corporate resources. |

**Security Incident Management, E-Discovery & Cloud Forensics**

| SEF-01 | Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement. | X | Google monitors a variety of communication channels for security incidents, and Google’s security personnel will react promptly to known incidents. |
| SEF-01.1 | Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? | X | Google maintains incident response procedures to help ensure prompt notification and investigation of incidents. |
| SEF-02.1 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures. | X | 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. |
| SEF-02.2 | Do you have a documented security incident response plan? | X | Google will respect the contractually agreed terms for customers in regards to incident notification. |
| SEF-02.3 | Do you have a policy that requires BYOD users to use anti-malware software (where supported)? | X | Please see Google’s Data Incident Response Whitepaper that details Google’s standard process for responding to incidents - https://cloud.google.com/security/incident-response/ |
| SEF-02.4 | Do you maintain automated log collection and analysis tools that collect and correlate log information from various sources? | X | Google’s Terms of Service cover roles and responsibilities. https://cloud.google.com/terms/ |
| SEF-03.1 | Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations. | X | Google performs annual testing of its emergency response processes. |
| SEF-03.3 | Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls? | X | Google maintains automated log collection and analysis tools that support the investigation of incidents on a per tenant basis. |
| SEF-04.1 | Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation. | X | Google can support properly formed requests for specific tenant data when requested by law enforcement. |
| SEF-04.2 | Does your response plan comply with the use of legally admissible forensic data collection and analysis techniques? | X | Google can support properly formed requests for specific tenant data when requested by law enforcement. |
| SEF-04.3 | Are you capable of supporting litigation holds (freeze of data) for a specific point in time? | X | Google Cloud Platform customers may implement this feature with external products or by using the “Bucket Lock” features available in Cloud Storage. G Suite customers may purchase Vault for their domain, which allows an organization to create retention/litigation holds without impacting other tenants. |
| SEF-04.4 | Do you have a policy that requires BYOD users to use anti-malware software (where supported)? | X | Google can support properly formed requests for specific tenant data when requested by law enforcement. |
Google reviews and analyzes security incidents to determine impact, cause, and opportunities for corrective action. Will you share statistical information for security incident data with your tenants upon request? X The amount of security incident data is currently statistically insignificant small. Should the amount of data increase, Google will consider sharing this statistical information.

Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.


Google collects capacity and use data on its infrastructure as needed to inform capacity planning and internal SLA performance.


Do you monitor and quantify the types, volumes, and costs of information security incidents? Do you collect and use data for all relevant components of your cloud service offering? Do you provide tenants with capacity planning and use reports? Do you provide the client with a list and copies of all (tenant) data impacted? Do you select and monitor outsourced providers in the organization being assessed? Do you review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner’s cloud supply chain?

Google does not depend on supply-chain partners for data quality.

Google maintains an internal program to assess ongoing conformance with relevant policies, as well as IT governance and service management policies and procedures. Does legal counsel review all third-party agreements? Does third-party agreements include provision for the security and protection of information and assets? Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?

Google employed a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.

Google’s agreements with subprocessors are subject to applicable laws and regulations.
The customer terms of services are updated as needed.

Do you have external third party services conduct vulnerability assessments?  

Do you review all agreements, policies and processes at least annually?  

Supply Chain Management, Transparency and Accountability  
Third Party Assessment  

Google employs a vendor management process that includes contractual requirements to adhere to Google’s security policies and onsite inspections, as needed, to confirm compliance.

Google permits customers to conduct their own vulnerability scans and penetration tests. In addition, Google maintains a robust bug bounty program and encourages input from the security community. For details see: http://www.google.com/about/appsecurity/reward-program/

Supply Chain Management, Transparency and Accountability  
Third Party Audits

Google permits customers to conduct their own vulnerability scans and penetration tests. In addition, Google maintains a robust bug bounty program and encourages input from the security community. For details see: http://www.google.com/about/appsecurity/reward-program/

Supply Chain Management, Transparency and Accountability  
Third Party Audits

Google permits customers to conduct their own vulnerability scans and periodic penetration tests. In addition, Google maintains a robust bug bounty program and encourages input from the security community. For details see: http://www.google.com/about/appsecurity/reward-program/

Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?

Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?

Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?

Do you review all agreements, policies and processes at least annually?

Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?

Google operates a robust bug bounty program and encourages input from the security community. For details see: http://www.google.com/about/appsecurity/reward-program/

Do you perform network-layer vulnerability scans regularly as prescribed by industry best practices?

Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?

Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?

Will you provide your risk-based systems patching time frames to your tenants upon request?

Google currently patches systems as needed and as quickly as vulnerabilities are addressed rather than on a scheduled basis. The notification process is determined in the terms of service and security guides.

https://cloud.google.com/security/whitepaper
https://cloud.google.com/terms/

Are you in compliance with Google’s Mobile Code policy?

Is mobile code authorized before its installation and execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?
Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

Is all unauthorized mobile code prevented from executing?  X  Google Cloud does not rely on mobile code.