<table>
<thead>
<tr>
<th>Control Domain</th>
<th>Control ID</th>
<th>Question ID</th>
<th>Control Specification</th>
<th>Consensus Assessment Questions</th>
<th>Consensus Assessment Answers</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application &amp; Interface Security</td>
<td>AIS-01</td>
<td>AIS-01.1</td>
<td>Applications and programming interfaces (APIs) shall be designed, developed, analyzed, and tested in accordance with leading industry standards (e.g., NIST 800-53 for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.</td>
<td>Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27334) to build in security for your systems/Software Development Lifecycle (SDLC) security?</td>
<td>X</td>
<td>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.</td>
</tr>
<tr>
<td>Application Security</td>
<td>AIS-01</td>
<td>AIS-01.2</td>
<td>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, corruption of data, or misuse?</td>
<td>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, corruption of data, or misuse?</td>
<td>X</td>
<td>Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access. (SaaS only) Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC)?</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>AIS-02</td>
<td>AIS-02.1</td>
<td>Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.</td>
<td>Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and mandated prior to granting customers access to data, assets, and information systems?</td>
<td>X</td>
<td>Sailors must agree to Google's Terms of Service and Acceptable Use Policy prior to using Google Cloud. Please see <a href="https://cloud.google.com/terms/">https://cloud.google.com/terms/</a> for current terms relating to Google Cloud Platform and G Suite products.</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>AIS-02</td>
<td>AIS-02.2</td>
<td>Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interface and databases to prevent manual or systematic processing errors, corruption of data, or misuse.</td>
<td>Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?</td>
<td>X</td>
<td>Customers are responsible for managing these types of features in their applications in Google Cloud's environment. Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access. Google is responsible for managing these types of features in their applications in Google Cloud's environment.</td>
</tr>
<tr>
<td>Application &amp; Interface Security</td>
<td>AIS-03</td>
<td>AIS-03.1</td>
<td>Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interface and databases to prevent manual or systematic processing errors, corruption of data, or misuse.</td>
<td>Are data input and output integrity routines (i.e., MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?</td>
<td>X</td>
<td>customers must agree to Google's Terms of Service and Acceptable Use Policy prior to using Google Cloud. Please see <a href="https://cloud.google.com/terms/">https://cloud.google.com/terms/</a> for current terms relating to Google Cloud Platform and G Suite products.</td>
</tr>
<tr>
<td>Application Security</td>
<td>AIS-03</td>
<td>AIS-03.2</td>
<td>Are all requirements and trust levels for customers' access defined and documented?</td>
<td>Are all requirements and trust levels for customer access contractually addressed and mandated prior to granting customers access to data, assets, and information systems?</td>
<td>X</td>
<td>Customers must agree to Google’s Terms of Service and Acceptable Use Policy prior to using Google Cloud. Please see <a href="https://cloud.google.com/terms/">https://cloud.google.com/terms/</a> for current terms relating to Google Cloud Platform and G Suite products.</td>
</tr>
<tr>
<td>Application Security</td>
<td>AIS-03</td>
<td>AIS-03.3</td>
<td>Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interface and databases to prevent manual or systematic processing errors, corruption of data, or misuse.</td>
<td>Are data input and output integrity routines (i.e., MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?</td>
<td>X</td>
<td>Customers must agree to Google’s Terms of Service and Acceptable Use Policy prior to using Google Cloud. Please see <a href="https://cloud.google.com/terms/">https://cloud.google.com/terms/</a> for current terms relating to Google Cloud Platform and G Suite products.</td>
</tr>
</tbody>
</table>
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 business functions to prevent improper disclosure, alteration, or destruction.

Is your Data Security Architecture designed using an industry standard (e.g., CSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, HABM, CASAFI)?

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 develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources) for reviewing the efficiency and effectiveness of implemented security controls?

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 conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?

AAC-02.2
Do you conduct network penetration tests of your cloud service infrastructure at least annually?

AAC-02.3
Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?

AAC-02.4
Do you conduct internal audits at least annually?

AAC-02.5
Do you conduct independent audits at least annually?

AAC-02.6
Are the results of the penetration tests available to tenants at their request?

AAC-02.7
Are the results of internal and external audits available to tenants at their request?

AAC-04.1
Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture addresses industry standards such as PCI-DSS, NIST 800-53, AICPA Trust Services Criteria (SOC2), and ISO/IEC 27001 security objectives.

AAC-01.1
Google maintains and implements comprehensive internal and external audit plans that are performed at least annually to test the efficiency and effectiveness of implemented security controls against recognized standards such as PCI-DSS, NIST 800-53, AICPA Trust Services Criteria (SOC2), and ISO/IEC 27001 security objectives.

AAC-02.1
Google makes its SOC2, ISO/IEC 27001 and similar third-party audit or certification reports available to customers.

AAC-02.2
Google conducts rigorous internal continuous testing of its network infrastructure through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers at least annually.

AAC-02.3
Google maintains an internal audit program consistent with industry best practices and regulatory requirements.

AAC-02.4
Google is committed to maintaining a program where independent verification of security, privacy, and compliance controls are regularly reviewed. 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/IEC 27001
ISO/IEC 27017 / 27018
PCI-DSS
HIPAA
For a full list of available certificates and compliance materials, please refer to: https://cloud.google.com/security/compliance

AAC-02.5
Google's Security Policy prohibits sharing this information but customers may conduct their own testing of our products and services.

AAC-02.6
Google's Security Policy prohibits sharing this information but customers may conduct their own testing of our products and services.

AAC-02.7
Google maintains and implements comprehensive internal and external audit plans that are performed at least annually to test the efficiency and effectiveness of implemented security controls against recognized standards such as PCI-DSS, NIST 800-53, AICPA Trust Services Criteria (SOC2), and ISO/IEC 27001 security objectives.

AAC-01.1
Does your audit program take into account effectiveness of implementation of security operations?

AAC-02.2
Does your audit program take into account effectiveness of implementation of security operations?

AAC-02.3
Does your audit program take into account effectiveness of implementation of security operations?

AAC-02.4
Does your audit program take into account effectiveness of implementation of security operations?

AAC-02.5
Does your audit program take into account effectiveness of implementation of security operations?

AAC-02.6
Does your audit program take into account effectiveness of implementation of security operations?

AAC-02.7
Does your audit program take into account effectiveness of implementation of security operations?
Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, conduct your security program for changes in legal requirements, and ensure compliance with relevant regulatory requirements?

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.

You automatically replicate to and serve data from multiple data centers to provide seamless access to end-users should a datacenter not be available.

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

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.

Google has implemented environmental controls, fail-over mechanisms and other redundancies for all its data centers throughout the world based on geographic region, Business Continuity/Disaster Recovery plans, and environmental factors to ensure that all utility services can operate based on our agreed upon Service Level Agreement (SLA)/Service Level Objective (SLO) in case of adverse environmental conditions.
BCR-04

BCR-04.1

Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:

• Configuring, installing, and operating the information system
• Effectively using the system's security features

Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?

X

Google performs annual testing of its business continuity plans to simulate disaster scenarios that model catastrophic events that may disrupt Google operations.

BCR-05

BCR-05.1

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, volcanic activity, nuclear accident, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.

Is physical damage anticipated and are countermeasures included in the design of physical protections?

X

Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threats. The video below provides an overview of our countermeasures:

https://www.youtube.com/watch?v=yfF3pOzdmlE

Additional resources:

a) Appendix 2 of Google Cloud’s Data Processing and Security Terms describe the security measures that Google will implement and maintain:
   https://cloud.google.com/terms/data-processing-terms#appendix-2:-security-measures
b) Google Cloud Security White Paper for details on our data center security:
   https://cloud.google.com/security/overview/whitepaper#technology_with_security_at_its_core
c) Information on Data Center Security:

BCR-06

BCR-06.1

To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.

Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?

X

Google carefully selects the locations of its datacenters to avoid exposure to high-impact environmental risks to the extent possible.

BCR-07

BCR-07.1

Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.

Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?

X

Google has dedicated teams and documented policies and procedures for all equipment in datacenters and routinely performs maintenance on that equipment. Additional resources:

a) Appendix 2 of Google Cloud’s Data Processing and Security Terms describe the security measures that Google will implement and maintain:
   https://cloud.google.com/terms/data-processing-terms#appendix-2:-security-measures
b) Google Cloud Security White Paper for details on our data center security:
   https://cloud.google.com/security/overview/whitepaper#technology_with_security_at_its_core
c) Information on Data Center Security:

BCR-07.2

Do you have an equipment and datacenter maintenance routine or plan?

X

Google has equipment and datacenter maintenance plans that it routinely reviews and performs.
**BCR-08.1** Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment. Any security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)? X Google has implemented redundancies and safeguards in its datacenters to minimize the impact of service outages.

**BCR-09.1** 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
- Determine impacts resulting from planned or unplanned disruptions and how these vary over time
- Establish the maximum tolerable period for disruption
- Establish priorities for recovery
- Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption

Do you use industry standards and frameworks to determine the impact of any disruptions to your organization (e.g. criticality of services and recovery priorities, disruption tolerance, RPO and RTO, etc.)? X Google uses widely accepted industry standards (such as NIST 800-53, ISO/IEC 27001/27017/27018, PO-IS, SOX 1/2/3 controls) and frameworks to determine the impact of disruptions.

**BCR-10.1** Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.

Are policies and procedures established and made available for all personnel to adequately support services operations’ roles? X Engineering teams maintain playbooks to facilitate the rapid reconstitution of services.

**BCR-11.1** Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.

Do you have technical capabilities to enforce tenant data retention policies? X 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/storing-your-data https://cloud.google.com/storage/docs/bucket-lock

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

**BCR-11.2** Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements? X Customers are responsible for managing their data retention policies. Customers may leverage the features of our storage services. Please see product documentation for specifics. In addition, some customers may use Google Vault to define organizational retention periods.

**BCR-11.3** Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements? X Google builds multiple software and hardware redundancies into its systems to prevent permanent data loss. At appropriate, data is replicated across data centers and geographic regions. However, due to the nature of some product lines, customers must determine their own business and replication requirements.
GCE (Google Compute Engine) provides the ability to perform full or incremental snapshots (backups) of the entire hard disk.

Google employs a vendor management process that includes contractual requirements to adhere to Google’s security policies. Organizations shall follow a defined quality change control and testing process.

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

Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate operations and/or data center facilities have been pre-approved by the organization’s business leadership or other accountable business role or function.

Policies and procedures are in place for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities. The authorization to provision additional processing capacity is obtained through budget approvals and managed through internal Service Level Agreements (SLAs) as part of an effective resource economy.

Are there policies and procedures in place for triage and remedy reported bugs and security vulnerabilities for product and service offerings?

If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?

Google embeds redundancy as part of its architecture and failure is expected and corrected continuously. Google annually performs continuous post-production tests based on real-time threats.
Do you have controls in place to detect source code security defects for any outsourced software development activities?  

| X | Google employs a vendor management process that includes contractual requirements to adhere to Google’s security, service level agreement and unacceptable operation, as needed, to confirm compliance. |

The mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?  

| X | Google follows a structured code development and release process. As part of this process, all code is peer reviewed, Google maintains robust build and code analysis tool available for to deploy against application code. Google also performs continuous post-production tests based on real-time threats. |

Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?  

| X | Google uses automated configuration management tools, software release tools, and mobile device management software to restrict and monitor the installation of unauthorized software. |

Do you have policies and procedures established for managing risks with respect to change management in production environments?  

| X | Google has a robust change management process and security policy that is documented and requires approval from appropriate stakeholders before being implemented into production. Google maintains a process to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. |

Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?  

| X | Google performs a robust change management process that is documented and requires approval from relevant stakeholders before being implemented into production. Google maintains a process to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. |

Do you have controls in place to restrict and monitor the installation of unauthorized software on organizationally-owned or managed user end-points?  

| X | Google follows a structured code development and release process. As part of this process, all code is peer reviewed, Google maintains robust build and code analysis tool available for to deploy against application code. Google also performs continuous post-production tests based on real-time threats. |

Do you have controls in place to restrict and monitor the installation of unauthorized software onto any systems?  

| X | Google uses automated configuration management tools, software release tools, and mobile device management software to restrict and monitor the installation of unauthorized software. |

Do you have policies and procedures established for managing the risks associated with the 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 shared with other third parties to ascertain any regulatory, statutory, or contractual compliance impact?  

| X | Google customers bring their own change and configuration management tools to Google Cloud. The customer is responsible for their own change management processes, including defining appropriate roles and responsibilities. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also follows a structured code development and release process. As part of this process, all code is peer reviewed, Google maintains robust build and code analysis tool available for to deploy against application code. Google also performs continuous post-production tests based on real-time threats. Google has a robust change management process and security policy that is documented and requires approval from appropriate stakeholders before being implemented into production. Google maintains a process to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. |

Do you have technical measures implemented to provide assurance that all unauthorized software on organizationally-owned or managed user end-points is detected, prevented and/or stopped?  

| X | Google follows a structured code development and release process. As part of this process, all code is peer reviewed, Google maintains robust build and code analysis tool available for to deploy against application code. Google also performs continuous post-production tests based on real-time threats. Google has a robust change management process and security policy that is documented and requires approval from appropriate stakeholders before being implemented into production. Google maintains a process to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. |

Do you provide tenants with documentation that describes your production change management procedures and their ownership/responsibility, within 60 days?  

| X | Google provides tenants with documentation that describes our production change management procedures and their ownership/responsibility. |

Do you have policies and procedures established for managing risks associated with the data? Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is shared with other third parties to ascertain any regulatory, statutory, or contractual compliance impact?  

| X | Google customers bring their own change and configuration management tools to Google Cloud. The customer is responsible for their own change management processes, including defining appropriate roles and responsibilities. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also follows a structured code development and release process. As part of this process, all code is peer reviewed, Google maintains robust build and code analysis tool available for to deploy against application code. Google also performs continuous post-production tests based on real-time threats. Google has a robust change management process and security policy that is documented and requires approval from appropriate stakeholders before being implemented into production. Google maintains a process to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. |

Do you have controls in place to restrict and monitor the installation of unauthorized software on any systems?  

| X | Google uses automated configuration management tools, software release tools, and mobile device management software to restrict and monitor the installation of unauthorized software. |

Do you have policies and procedures established for managing the risks associated with the data? Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is shared with other third parties to ascertain any regulatory, statutory, or contractual compliance impact?  

| X | Google customers bring their own change and configuration management tools to Google Cloud. The customer is responsible for their own change management processes, including defining appropriate roles and responsibilities. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also follows a structured code development and release process. As part of this process, all code is peer reviewed, Google maintains robust build and code analysis tool available for to deploy against application code. Google also performs continuous post-production tests based on real-time threats. Google has a robust change management process and security policy that is documented and requires approval from appropriate stakeholders before being implemented into production. Google maintains a process to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. |

Do you have policies and procedures established for managing the risks associated with the data? Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is shared with other third parties to ascertain any regulatory, statutory, or contractual compliance impact?  

| X | Google customers bring their own change and configuration management tools to Google Cloud. The customer is responsible for their own change management processes, including defining appropriate roles and responsibilities. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also follows a structured code development and release process. As part of this process, all code is peer reviewed, Google maintains robust build and code analysis tool available for to deploy against application code. Google also performs continuous post-production tests based on real-time threats. Google has a robust change management process and security policy that is documented and requires approval from appropriate stakeholders before being implemented into production. Google maintains a process to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle). Every Google Cloud product maintains a well documented release and deployment process. This process is validated for each product during the semi-annual compliance audit cycle. |

Do you have controls in place to restrict and monitor the installation of unauthorized software on any systems?  

| X | Google uses automated configuration management tools, software release tools, and mobile device management software to restrict and monitor the installation of unauthorized software. |
Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing assets?

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 responsibilities regarding data stewardship shall be defined, documented, and communicated. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. Are policies and procedures established with supporting business processes and technical measures implemented, to inventory, document, and process data flows and applications and infrastructure network and systems components and/or shared with other third parties to assure 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 tenants of compliance impact and risk, especially if customer data is used as part of the service.

Do you provide standardized (e.g., ISO27001) non-proprietary encryption algorithms (AES, 3DES) for tenants in order for them to protect their data? It is required to use public networks (e.g., the internet)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are policies and procedures established for labeling, handling, archiving, and the security of data and applications which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

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)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing assets?

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 responsibilities regarding data stewardship shall be defined, documented, and communicated. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. Are policies and procedures established with supporting business processes and technical measures implemented, to inventory, document, and process data flows and applications and infrastructure network and systems components and/or shared with other third parties to assure 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 tenants of compliance impact and risk, especially if customer data is used as part of the service.

Do you provide standardized (e.g., ISO27001) non-proprietary encryption algorithms (AES, 3DES) for tenants in order for them to protect their data? It is required to use public networks (e.g., the internet)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are policies and procedures established for labeling, handling, archiving, and the security of data and applications which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

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)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing assets?

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 responsibilities regarding data stewardship shall be defined, documented, and communicated. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. Are policies and procedures established with supporting business processes and technical measures implemented, to inventory, document, and process data flows and applications and infrastructure network and systems components and/or shared with other third parties to assure 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 tenants of compliance impact and risk, especially if customer data is used as part of the service.

Do you provide standardized (e.g., ISO27001) non-proprietary encryption algorithms (AES, 3DES) for tenants in order for them to protect their data? It is required to use public networks (e.g., the internet)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are policies and procedures established for labeling, handling, archiving, and the security of data and applications which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

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)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing assets?

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 responsibilities regarding data stewardship shall be defined, documented, and communicated. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. Are policies and procedures established with supporting business processes and technical measures implemented, to inventory, document, and process data flows and applications and infrastructure network and systems components and/or shared with other third parties to assure 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 tenants of compliance impact and risk, especially if customer data is used as part of the service.

Do you provide standardized (e.g., ISO27001) non-proprietary encryption algorithms (AES, 3DES) for tenants in order for them to protect their data? It is required to use public networks (e.g., the internet)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are policies and procedures established for labeling, handling, archiving, and the security of data and applications which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

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)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing assets?

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 responsibilities regarding data stewardship shall be defined, documented, and communicated. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. Are policies and procedures established with supporting business processes and technical measures implemented, to inventory, document, and process data flows and applications and infrastructure network and systems components and/or shared with other third parties to assure 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 tenants of compliance impact and risk, especially if customer data is used as part of the service.

Do you provide standardized (e.g., ISO27001) non-proprietary encryption algorithms (AES, 3DES) for tenants in order for them to protect their data? It is required to use public networks (e.g., the internet)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are policies and procedures established for labeling, handling, archiving, and the security of data and applications which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

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)?

Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, USA data type guidelines)?

Are you responsible for data labeling, defined, assigned, communicated, and documented?

Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?

Are you responsible for data labeling, defined, assigned, communicated, and documented?
Do you maintain a complete inventory of all of your critical assets located at all site(s) or geographical locations and their assigned ownership? X

Google maintains asset inventories and assigns ownership for managing its critical resources.

Physical security perimeters (e.g., fences, walls, barriers, guards, 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, guards, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas having sensitive data and information systems? X

Google Data Centers maintain secure external perimeter protections. All data centers employ electronic card key access control systems that are linked to a system alarm. Access to perimeter doors, shipping, and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on an individual's job responsibilities. The fire doors of 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 patrols are in operation both inside and outside the data centers with camera-based or manual control of the equipment. Access to the perimeter doors is alarmed and can only be opened from the inside.

Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises? X

Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises. Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? X

Google uses certificates and access control lists (ACLs) to achieve authentication integrity. Location-aware technologies may be used to validate authentication. Google uses certificates and ACLs to achieve authentication integrity. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.

Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies and procedures? X

Google trains its employees and contractors annually as part of their contract. Third-party contractors agree to observe Google's security policies as part of their contract.

Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies and procedures? X

Google trains its employees and contractors annually as part of their contract. Third-party contractors agree to observe Google's security policies as part of their contract.

Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain, and monitor access to physical access control mechanisms? X

A combination of CCTV cameras, ID cards, entry controls, mantraps, and gate checkpoints are used to monitor ingress and egress at the various physical security zones in a Data Center.
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 opened only 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 vital digital video recorders 24 hours a day, 7 days a week.
Google employs several security measures to help ensure the authenticity, integrity, and privacy of data in transit.

Google maintains documentation for the use of its internal proprietary key management service.

Google has automated mechanisms to detect deviations from the desired security configuration of its infrastructure.

Managers are responsible for maintaining awareness of, and complying with, Google’s security policies, procedures, and standards that are relevant to their area of responsibility.

Are you leverage encryption to protect data and virtual machine images during transport across and between networks and virtualization infrastructure?

Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?

Are you encryption keys maintained by the cloud consumer or entrusted key management provider?

Do you leverage encryption in the cloud to protect data in transit?

Do you have separate key management and key usage duties?

Do you conduct risk assessments associated with data governance requirements at least once a year?

Do you have documented information security baselines for every component of your infrastructure e.g., hypervisors, operating systems, routers, DNS servers, etc.?

Do you have policies and procedures for data classification and protection from unauthorized use, access, disclosure, alteration, and destruction insofar as they relate to the characteristics of the business?

Are your encryption keys maintained by the cloud consumer or a trusted key management provider?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you leverage encryption to protect data and virtual machine images during transport across and between networks and virtualization infrastructure?

Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?

Are you encryption keys maintained by the cloud consumer or entrusted key management provider?

Do you leverage encryption in the cloud to protect data in transit?

Do you have separate key management and key usage duties?

Do you conduct risk assessments associated with data governance requirements at least once a year?

Do you have documented information security baselines for every component of your infrastructure e.g., hypervisors, operating systems, routers, DNS servers, etc.?

Do you have policies and procedures for data classification and protection from unauthorized use, access, disclosure, alteration, and destruction insofar as they relate to the characteristics of the business?

Are your encryption keys maintained by the cloud consumer or a trusted key management provider?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you leverage encryption to protect data and virtual machine images during transport across and between networks and virtualization infrastructure?

Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?

Are you encryption keys maintained by the cloud consumer or entrusted key management provider?

Do you leverage encryption in the cloud to protect data in transit?

Do you have separate key management and key usage duties?

Do you conduct risk assessments associated with data governance requirements at least once a year?

Do you have documented information security baselines for every component of your infrastructure e.g., hypervisors, operating systems, routers, DNS servers, etc.?

Do you have policies and procedures for data classification and protection from unauthorized use, access, disclosure, alteration, and destruction insofar as they relate to the characteristics of the business?

Are your encryption keys maintained by the cloud consumer or a trusted key management provider?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you leverage encryption to protect data and virtual machine images during transport across and between networks and virtualization infrastructure?

Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?

Are you encryption keys maintained by the cloud consumer or entrusted key management provider?

Do you leverage encryption in the cloud to protect data in transit?

Do you have separate key management and key usage duties?

Do you conduct risk assessments associated with data governance requirements at least once a year?

Do you have documented information security baselines for every component of your infrastructure e.g., hypervisors, operating systems, routers, DNS servers, etc.?

Do you have policies and procedures for data classification and protection from unauthorized use, access, disclosure, alteration, and destruction insofar as they relate to the characteristics of the business?

Are your encryption keys maintained by the cloud consumer or a trusted key management provider?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you leverage encryption to protect data and virtual machine images during transport across and between networks and virtualization infrastructure?

Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?

Are you encryption keys maintained by the cloud consumer or entrusted key management provider?

Do you leverage encryption in the cloud to protect data in transit?

Do you have separate key management and key usage duties?

Do you conduct risk assessments associated with data governance requirements at least once a year?

Do you have documented information security baselines for every component of your infrastructure e.g., hypervisors, operating systems, routers, DNS servers, etc.?

Do you have policies and procedures for data classification and protection from unauthorized use, access, disclosure, alteration, and destruction insofar as they relate to the characteristics of the business?

Are your encryption keys maintained by the cloud consumer or a trusted key management provider?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?

Do you leverage encryption to protect data and virtual machine images during transport across and between networks and virtualization infrastructure?

Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?

Are you encryption keys maintained by the cloud consumer or entrusted key management provider?

Do you leverage encryption in the cloud to protect data in transit?

Do you have separate key management and key usage duties?

Do you conduct risk assessments associated with data governance requirements at least once a year?

Do you have documented information security baselines for every component of your infrastructure e.g., hypervisors, operating systems, routers, DNS servers, etc.?
| GRM-04.2 | Information security policies and procedures should be established and made accessible to all employees. What actions do you take to ensure compliance? | X | Google reviews its GMS documentation annually as part of its required due diligence. |
| GRM-05.1 | Are information security policies authorized by the organization’s business leadership (or other accountable business role or function)? | X | Google executive management reviews and approves all information security policies and sets applicable commitment and direction to achieve the agreed upon Information Security goals. |
| GRM-06.1 | Information security policies and procedures shall be established and made accessible to all employees. What actions do you take to ensure compliance? | X | Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified GMS, roles and responsibilities are documented and authorized by leadership. |
| GRM-07.1 | 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. |
| GRM-08.1 | Do executive and line management take formal action to support information security through clearly documented direction and responsibilities for business leadership? | X | Google makes its internal policies available to all personnel. Communication of policies occurs via required training, and records of certification are retained to ensure compliance. |
| GRM-09.1 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | X | Google’s guide to internal policies is available at https://abc.xyz/investor/other/code-of-conduct/ |
| GRM-10.1 | Do you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-11.1 | Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by 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? | X | Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified GMS, roles and responsibilities are documented and authorized by leadership. |
| GRM-12.1 | 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. |
| GRM-13.1 | Do you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-14.1 | Can you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-15.1 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | X | Google’s guide to internal policies is available at https://abc.xyz/investor/other/code-of-conduct/ |

**Governance and Risk Management Policy**

| GRM-06.1 | Information security policies and procedures shall be established and made accessible to all employees. What actions do you take to ensure compliance? | X | Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified GMS, roles and responsibilities are documented and authorized by leadership. |
| GRM-07.1 | 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. |
| GRM-08.1 | Do executive and line management take formal action to support information security through clearly documented direction and responsibilities for business leadership? | X | Google makes its internal policies available to all personnel. Communication of policies occurs via required training, and records of certification are retained to ensure compliance. |
| GRM-09.1 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | X | Google’s guide to internal policies is available at https://abc.xyz/investor/other/code-of-conduct/ |
| GRM-10.1 | Do you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-11.1 | Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by 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? | X | Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified GMS, roles and responsibilities are documented and authorized by leadership. |
| GRM-12.1 | 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. |
| GRM-13.1 | Do you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-14.1 | Can you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-15.1 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | X | Google’s guide to internal policies is available at https://abc.xyz/investor/other/code-of-conduct/ |

**Governance and Risk Management Policy**

| GRM-06.1 | Information security policies and procedures shall be established and made accessible to all employees. What actions do you take to ensure compliance? | X | Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified GMS, roles and responsibilities are documented and authorized by leadership. |
| GRM-07.1 | 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. |
| GRM-08.1 | Do executive and line management take formal action to support information security through clearly documented direction and responsibilities for business leadership? | X | Google makes its internal policies available to all personnel. Communication of policies occurs via required training, and records of certification are retained to ensure compliance. |
| GRM-09.1 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | X | Google’s guide to internal policies is available at https://abc.xyz/investor/other/code-of-conduct/ |
| GRM-10.1 | Do you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-11.1 | Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by 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? | X | Google maintains a robust and up-to-date Information Security Management System that is audited at least yearly and signed off by business leadership. As part of the ISO/IEC 27001 certified GMS, roles and responsibilities are documented and authorized by leadership. |
| GRM-12.1 | 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. |
| GRM-13.1 | Do you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-14.1 | Can you provide evidence of due diligence in managing your controls, architecture, and processes to ensure regulatory and/or standards compliance? | X | Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained. |
| GRM-15.1 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | X | Google’s guide to internal policies is available at https://abc.xyz/investor/other/code-of-conduct/ |
Google maintains personnel and data access policies that govern the administration of access controls including transfers of workforce personnel user access to corporate facilities, resources, and assets.

Google's risk assessment considers inherent and residual risk factors as part of its review process. 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.

Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations. 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 organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as needed.

Google has a well defined process including equipment return procedures for terminated personnel. Exit checklists are provided to both personnel and their managers to inform them of their obligations for returning organizationally-owned assets.

Google's risk management program includes the following components:

- Risk identification
- Risk analysis (threat and vulnerability analysis, and regulatory compliance)
- Risk evaluation (likelihood and impact associated with inherent and residual risk)
- Risk treatment (actions to mitigate risk)
- Risk monitoring (ongoing evaluation of risk)

Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?

Do you have documented, organization-wide procedures to manage risk?

Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?

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

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

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

Do you have asset return procedures outlining how assets should be returned within an established period?

Do you have documented policies, procedures, and guidelines in place to govern change in employment and/or termination?

Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?
Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required by our personnel policies. Google maintains a security awareness program for its personnel. Customers are responsible for training their users.

- Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, and acceptable-use policies and procedures (e.g., mandated security training, IT infrastructure network and systems components)?
- Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?
- Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?
- Do you define availability and conditions for RHIO devices and its applications to access corporate resources?
- Google's Terms of Service outline the responsibilities of Google and customers.
- Are personnel trained and provided with awareness programs at least once a year?
- Are personnel required to acknowledge the training they have completed?
- Do you review NDA and confidentiality documents as needed?
- Google has a Code of Conduct and Information Security Policy that governs the usage of devices at Google.
- Google has well-defined Mobile Device Management Policy that governs and defines the allowances and conditions for the use of corporate services. RHIO devices must meet specific requirements including the deployment of a corporate policy that enforces the same rules and allows for the remote wipe of corporate data.
Google maintains an automated access revocation process that includes account locking and revocation of certificates and keys. Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)? X

Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents? X

Does Google have a well-established security policy that requires all personnel to store sensitive materials out of sight? X

Google restricts access based on need-to-know and job function. Do you monitor and log privileged access (e.g., administrator level) to information security management systems? X

Google maintains automated log collection and analysis tools. Multi-factor authentication is required for any connections to your production environment. Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege? X

Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools. Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes? X

Google restricts access based on need-to-know and job function in accordance with applicable legal and compliance requirements. Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures? X

Google restricts access based on need-to-know and job function. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege? X

Google restricts access based on need-to-know and job function. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)? X

Google maintains policies and procedures that enforce data access permissions. Two factor authentication is required for privileged access to all company and customer resources. Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in multi-tenant architectures? X

Google maintains policies and procedures that enforce data access permissions. Two factor authentication is required for privileged access to all company and customer resources. Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business use cases, supported by multi-factor authentication? X
| IAM-02.7 | Does your organization conduct third-party unauthorized access risk assessments? | X | Google's periodic risk assessments do address the risks of unauthorized access by insiders and third-parties. |
| Identity & Access Management | Responsibilities | IAM-02.1 | User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications. | Google restricts access based on need-to-know and job function. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. |
| Identity & Access Management | Policies and Procedures | IAM-06.1 | 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. | Google restricts access based on need-to-know and job function. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. |
| Identity & Access Management | Responsibilities | IAM-05.1 | User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications. | Google restricts access based on need-to-know and job function. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. |
| Identity & Access Management | Policies and Procedures | IAM-04.1 | 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. | Google restricts access based on need-to-know and job function. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. |
| Identity & Access Management | Responsibilities | IAM-06.1 | User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications. | Google restricts access based on need-to-know and job function. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. |
| Identity & Access Management | Policies and Procedures | IAM-04.1 | 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. | Google restricts access based on need-to-know and job function. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. |
Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically evaluates its access lists and removes access that is no longer required. All account actions are recorded.

Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?

Do you monitor and manage user access promptly and proactively to ensure unauthorized access to data is prevented?

By whom is the responsibility for investigating access violations and reviewing access policies and procedures managed?

Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?

Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusion of users monitored by your tenant), based on the rule of least privilege, by business leadership or other accountable business role or function?

Do you ensure that remediation actions for access violations follow user access policies?

Are preventive, detective, corrective, compensating controls in place to mitigate impacts of unauthorized or inappropriate access?

Google requires access reviews at least annually for critical access groups.

Is any change in user access status intended to include termination of employment, contract or agreement, change of other accountable business role or function?

Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (excluding of users monitored by your tenant), based on the rule of least privilege, by business leadership or other accountable business role or function?

Do you maintain customers' notification requirements that should their data and work with the customer in good faith to address any known breach of Google's security obligations?

Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?

Are you aware of the preventive, detective, corrective, compensating controls in place to mitigate impacts of unauthorized or inappropriate access?

Customer is responsible for configuring the access by their users to the service. For Google personnel, authorization is required prior to access being granted.

Are preventive, detective, corrective, compensating controls in place to mitigate impacts of unauthorized or inappropriate access?

Customers restrict access based on need-to-know and job function.

Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (excluding of users monitored by your tenant), based on the rule of least privilege, by business leadership or other accountable business role or function?

Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (excluding of users monitored by your tenant), based on the rule of least privilege, by business leadership or other accountable business role or function?

Do you implement access controls as per established policies and based on user's change in status?

Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (excluding of users monitored by your tenant), based on the rule of least privilege, by business leadership or other accountable business role or function?

Do you provide a copy of Google's 3rd party attestation reports, external audit reports for SOC 2 compliance is conducted.

Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?

Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?

Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (excluding of users monitored by your tenant), based on the rule of least privilege, by business leadership or other accountable business role or function?

Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (excluding of users monitored by your tenant), based on the rule of least privilege, by business leadership or other accountable business role or function?
Identity & Access Management

IAM-12.2
Client access management and in accordance with established policies and authorities:

• 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 identity store minimization or re-use when feasible
• Reference to industry acceptable and/or regulatory compliant authorization, authentication, and accounting (AAA) rules (e.g., strong/multi-factor, exotic, non-shared authentication secrets)

Do you use open standards to delegate authentication capabilities to your tenants?

X

Google supports open standards such as OAuth, OpenID, and SAML 2.0.

IAM-12.3
Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?

X

Google supports SAML as a means for authenticating users.

IAM-12.4
Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?

X

Google Cloud Identity & Access Management (IAM) lets administrators authorize who can take action on specific resources, using full control and flexibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups and potentially many more projects, Cloud IAM provides a unified view into security policy across the entire organization, with built-in auditing to ease compliance procedures. IAM access policies are defined at the project level using granular controls of users and groups or using ACLs.

https://cloud.google.com/identity/
https://cloud.google.com/iam/
https://cloud.google.com/compute/docs/access/

IAM-12.5
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?

X

Customers can integrate authentication to their existing identity management system. Customers can customize access to data by organization and user and assign administrative access profiles based on roles.

Google provides customers with additional tooling to gain more granular control over their access management solution:

https://cloud.google.com/iap/
https://cloud.google.com/context-aware-access/

IAM-12.6
Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?

X

Google provides the capability for domain administrators to enforce Google's 2-step verification. The 2nd factor could be a code generated by Google's Authenticator application or via a supported hardware key. Should a tenant choose to set up SSO against their own password management system, they would be able to leverage any third-party multifactor option that their system supports.

IAM-12.7
Do you allow tenants to use third-party identity assurance services?

X

Google supports integration with third-party identity assurance services.

IAM-12.8
Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?

X

Google native authentication requires a minimum 8 character complex password. Tenants can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the tenant whom can decide to force a password change on any user that is later detected to have a password that is weak. Google's native authentication has protections in place that would detect a brute force attack and challenge the user to solve a Captcha and would auto lock the account if suspicious activity is detected. The tenant's System Administrators can reset that account for the end user.

IAM-12.9
Do you allow tenants/customers to define password and account lockout policies for their accounts?

X

Custom policies can be enforced through SSO integration as a standard part of our offering.

IAM-12.10
Do you support the ability to force password changes upon first logon?

X

Google by default requires a password change upon first login.

 IAM-12.11
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)?

X

Administrators can manually lock and unlock accounts.

Identity & Access Management

Utility Programs

Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.

Utility programs used to manage virtualized partitions (e.g. shadow, clone, etc) appropriately isolated and monitored

Any access to utility programs used to manage virtualized partitions (e.g. shadow, clone, etc) appropriately isolated and monitored

IAM-13.1

Utility programs used to manage virtualized partitions (e.g. shadow, clone, etc) are appropriately isolated and monitored

X

IAM-13.2
Do you support open standards to delegate authentication capabilities to your tenants?

X

Google supports open standards such as OAuth, OpenID, and SAML 2.0.

IAM-13.3
Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?

X

Google supports SAML as a means for authenticating users.

IAM-13.4
Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?

X

Google Cloud Identity & Access Management (IAM) lets administrators authorize who can take action on specific resources, using full control and flexibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups and potentially many more projects, Cloud IAM provides a unified view into security policy across the entire organization, with built-in auditing to ease compliance procedures. IAM access policies are defined at the project level using granular controls of users and groups or using ACLs.

https://cloud.google.com/identity/
https://cloud.google.com/iam/
https://cloud.google.com/compute/docs/access/

IAM-13.5
Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?

X

Google provides the capability for domain administrators to enforce Google's 2-step verification. The 2nd factor could be a code generated by Google's Authenticator application or via a supported hardware key. Should a tenant choose to set up SSO against their own password management system, they would be able to leverage any third-party multifactor option that their system supports.

IAM-13.6
Do you allow tenants to use third-party identity assurance services?

X

Google supports integration with third-party identity assurance services.

IAM-13.7
Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?

X

Google native authentication requires a minimum 8 character complex password. Tenants can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the tenant whom can decide to force a password change on any user that is later detected to have a password that is weak. Google's native authentication has protections in place that would detect a brute force attack and challenge the user to solve a Captcha and would auto lock the account if suspicious activity is detected. The tenant's System Administrators can reset that account for the end user.

IAM-13.8
Do you allow tenants/customers to define password and account lockout policies for their accounts?

X

Custom policies can be enforced through SSO integration as a standard part of our offering.

IAM-13.9
Do you support the ability to force password changes upon first logon?

X

Google by default requires a password change upon first login.

IAM-13.10
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)?

X

Administrators can manually lock and unlock accounts.
Google has implemented network and host-based tools to detect and respond to potential security incidents. Google maintains an automated log collection and analysis tool to support investigations.

Google uses a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference.

Google maintains an automated log collection and analysis tool to review and analyzing events.

Google machine configuration changes are continuously monitored with automated tools.

Google restricts physical and logical access to audit logs.

Google maintains an effective resource economy with internal Service Level Agreements between engineering teams that provide for capacity planning and provisioning decisions.

Google has implemented efficient memory management techniques in the virtual machine system.

Google uses a centralized custom-built GRC system where compliance and regulatory standard mappings are maintained.

Google has implemented and network and host-based tools to detect and respond to potential security incidents. Google maintains an automated log collection and analysis tool to support investigations.

Google maintains automated log collection and analysis tool to review and analyzing events.

Google maintains an automated log collection and analysis tool to support investigations.

Google has implemented efficient memory management techniques in the virtual machine system.

Google has implemented efficient memory management techniques in the virtual machine system.
Google provides solution papers and reference docs for various architectures and intended solutions.

Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?

Network ACLs are documented within configuration files with comments on purpose, as appropriate.

Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: central user ID management, central authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.

Google performs fuzz testing, penetration testing, and vulnerability scanning to detect, mitigate, and resolve security issues.

Use system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements.

Do you regularly update network architecture diagrams that include data flows between security domains/zones?

The security state of network devices is monitored continuously.

Customers can use organizational structures with their environment to help manage segregation of sensitive data.

Network environments and virtual instances shall be designed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant environments.

Google builds its own machines and deploys custom operating system images that only permit the necessary ports, protocols, and services.

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?

Google employs multiple layers of network devices to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate defensive controls at its perimeter and boundaries.

For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?

Google maintains network diagrams for internal purposes, that are dynamic and updated regularly.

Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security environments across the network?

For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?

IVS-09.2

Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and in place supporting 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 can provision separate domains or organizations within a domain for testing purposes.

Customers can provision separate domains or organizations within a domain for testing purposes.

Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?

For your SaaS offering, do you provide customers with separate environments for production and test processes?

IVS-09.1

Google can provision separate domains or organizations within a domain for testing purposes.

For your IaaS offering, do you provide tenants with a guidance on how to create suitable production and test environments?

Network environments and virtual instances shall be designed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant environments.

Do your security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?

Google maintains network diagrams for internal purposes, that are dynamic and updated regularly.

Does your layered security architecture include a network firewall using your virtualized solution?

Do you regularly update network architecture diagrams that include data flows between security domains/zones?

Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and in place supporting technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline operating build standard or template.

Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security environments across the network?

For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?

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?

Google can provide solution papers and reference docs for development and test environments.

Do you regularly update network architecture diagrams that include data flows between security domains/zones?

Do you have the responsibility of the customer to deal with legal requests. Google will provide customers with assistance with these requests, if necessary.

For your SaaS offering, do you provide customers with separate environments for production and test processes?

Do you regularly update network architecture diagrams that include data flows between security domains/zones?

Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security environments across the network?

Google can provide solution papers and reference docs for development and test environments.

Do you regularly update network architecture diagrams that include data flows between security domains/zones?

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?

Google can provide solution papers and reference docs for development and test environments.

Do you regularly update network architecture diagrams that include data flows between security domains/zones?

Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and in place supporting technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline operating build standard or template.

Do you regularly update network architecture diagrams that include data flows between security domains/zones?

Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?

For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?

Do you regularly update network architecture diagrams that include data flows between security domains/zones?

Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and in place supporting technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline operating build standard or template.

For your SaaS offering, do you provide customers with separate environments for production and test processes?
Policies and procedures shall be established, and supporting business network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

Are you restricted from using a network segregated from production-level networks for such migrations?

Are you provided policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between applications (API) and information processing interoperability, and portability?

Are you provided policies and procedures (e.g. service level agreements) governing the use of APIs for interoperability between applications (API) and information processing interoperability, and portability?

Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?

Do you restrict personnel access to all supervisory management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, log addressing filtering, and unencrypted communications to the administrative console).

Do you maintain secure source code build tools to dynamically identify changes to the networks in real-time.

Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between applications (API) and information processing interoperability, and portability.

Are you provided policies and procedures (e.g. service level agreements) governing the use of APIs for interoperability between applications (API) and information processing interoperability, and portability?

Do you have a network segregated from production-level networks when migrating wireless servers, applications, or data to virtual environments?

Are you provided policies and procedures (e.g. service level agreements) governing the use of APIs for interoperability between applications (API) and information processing interoperability, and portability.

Are you provided policies and procedures (e.g. service level agreements) governing the use of APIs for interoperability between applications (API) and information processing interoperability, and portability.

Do you do your own network segmentation from production-level networks when migrating wireless servers, applications, or data to virtual environments?

Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?
Customers can export/import an entire VM image in the form of a .tar archive.

The Google Device Policy restricts the user and device behavior on mobile devices including application installation. For instance:

- IPY-04.1
- MOS-07.1
- MOS-09.1

A documented list of approved application stores has been communicated as IPY-04.1 MOS-07.1 MOS-09.1.

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

Google supports most virtual disk file formats, including VMDK, VHD and RAW.

The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., VDI) to help ensure interoperability and portability. "Interoperability & Portability" for each device in the inventory.

Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto mobile devices?

Google provides documentation regarding how customers may port data. Our GDPR resource site provides an entry point for each device in the inventory.

Do you have a BYOD policy and supporting awareness training clearly stating the acceptable usage and requirements for all mobile devices. The provider shall post and communicate to all personnel who are involved.

The BYOD policy and supporting awareness training clearly states the acceptable usage and requirements for all mobile devices. The provider shall post and communicate to all personnel who are involved.

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

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

Google supports security training to all employees and includes references to our security policies, including the BYOD policy.

The BYOD policy shall define the device and eligibility requirements to allow mobile devices permitted to store, transmit, or process company data?

Google supports security training to all employees and includes references to our security policies, including the BYOD policy.

Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto mobile devices?

Google uses the KVM hypervisor. Security enhancements made to the KVM hypervisor are documented here: https://cloud.google.com/blog/products/gcp/7-ways-we-harden-our-kvm-hypervisor-at-google-cloud-security-in-plaintext/#

The BYOD policy shall define the device and eligibility requirements to allow mobile devices permitted to store, transmit, or process company data?

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

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.

Google supports security 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.

Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto mobile devices?

The BYOD policy shall define the device and eligibility requirements to allow mobile devices permitted to store, transmit, or process company data?

Google supports security 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.

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

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.

Google supports security 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.

Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto mobile devices?

The BYOD policy shall define the device and eligibility requirements to allow mobile devices permitted to store, transmit, or process company data?

Google supports security 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.

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

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.

Google supports security 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.

Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto mobile devices?

The BYOD policy shall define the device and eligibility requirements to allow mobile devices permitted to store, transmit, or process company data?
The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive through technology controls on all mobile devices and shall

Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive through technology controls on all mobile devices and shall

Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?

Do you have detection and prevention controls on the device or use a centralized device management system which prohibit the circumvention of built-in security controls?

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

Mobile devices that do not permit jailbreaking or rooting on devices enabled to a Google corporate account.

Google's mobile device policy clearly states the expectations over the loss of non-company data in case a wipe of the device is required.

Google does not permit access to production data in mobile devices.

All mobile devices permitted for use through the company BYOD program or a

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

Do you require anti-malware software (where supported)?

Are your password policies enforced through technical controls (i.e. MDM)?

Are your password policies enforced through technical controls on all mobile devices (i.e. MDM)?

MOS-19.1

BYOD and/or company-owned devices are configured to require an automatic lockout screen in the event of an unauthorized login, and the requirement shall be enforced through technical controls.

Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, discovery, and legal hold?

Does the BYOD policy clearly state the expectation over the loss of non-company data in case a wipe of the device is required?

Google's mobile device policy clearly states the expectations over the loss of non-company data in case a wipe of the device is required.

Google's mobile device policy clearly states the expectations over the loss of non-company data in case a wipe of the device is required.

Google's mobile device policy clearly states the expectations over the loss of non-company data in case a wipe of the device is required.

Google requires mobile devices (including personally owned devices) to conform to corporate device management policies that require the installation of all updates and sets minimum O/S requirements. Google requires mobile devices (including personally owned devices) to conform to corporate device management policies that require the installation of all updates and sets minimum O/S requirements.

Google requires remote wipe capabilities for all mobile devices managed by Google.

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security

Mobile Security
Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security events?

SEF-04.1 Have you tested your security incident response plans in the last year?

Google can support properly formed requests for specific tenant data when requested by law enforcement.

Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?

Google has a well established privacy and information security training program that informs personnel of their responsibility to report security events in a timely manner.

Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?

Google maintains incident response procedures to help ensure prompt notification and investigation of incidents.

Do you perform annual testing of your emergency response processes.

Forensic procedures, including chain of custody, are required for the forensic investigation.

Does your incident response plan comply with industry standards for legally admissible chain-of-custody management?

Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without impacting other tenants?

Does your incident response plan comply with industry standards for legally admissible chain-of-custody management?

Does your incident response plan comply with industry standards for legally admissible chain-of-custody management?

Google will respect the contractually agreed terms for customers in regards to incident notification.

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 involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team.

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/

In the event of a data incident response process is described in this whitepaper: https://cloud.google.com/security/incident-response

Does your incident response plan comply with industry standards for legally admissible chain-of-custody management?

Does your incident response plan comply with industry standards for legally admissible chain-of-custody management?
Do you monitor and quantify the types, volumes, and impacts on all information security incidents?

Will you share statistical information for security incident data with your tenants upon request?

The amount of security incident data is currently statistically insignificantly small. Should the amount of data increase, Google will consider sharing this statistical information.

Do third-party agreements include provision for the security and protection of information and assets?

Google has a well-defined vendor management policy and process to select and monitor third-party providers. Google employs a vendor management process that includes contractual requirements to adhere to Google's security requirements and principles.

Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?

This falls under customer responsibility as they retain control and ownership over the quality of their data and potential liability errors that may arise through their usage of Google Cloud.

Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?

Google maintains an internal program to assess ongoing conformance with relevant policies, procedures, and metrics.

Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?

Google conducts ongoing audits of subprocessors for compliance. Third-party agreements go through multiple levels of review, including legal review by appropriate counsel.

Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?

Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?

Do you make security incident information available to all affected customers and providers periodically through electronic means (e.g., portal)?

Do you provide tenants with capacity planning and use reports?

Do you monitor and quantify the types, volumes, and impacts on all information security incidents?

Do third-party agreements include provision for the security and protection of information and assets?

Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?

Do you monitor and quantify the types, volumes, and impacts on all information security incidents?

Do third-party agreements include provision for the security and protection of information and assets?

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.

Do you monitor and quantify the types, volumes, and impacts on all information security incidents?

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.
| STA-05.1 | Do you have the capability to recover data for a specific customer in the case of a failure or data loss? | 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. [https://cloud.google.com/terms](https://cloud.google.com/terms) |
| STA-05.2 | Do you have the capability to restrict the storage of customer data to specific countries or geographic locations? | X | Customers can choose data locations in the UK and Europe when configuring some of their Google Cloud Platform services. If these locations are made among shared services, this is limited by the service specific terms within Google’s Terms of Service. |
| STA-05.3 | Can you provide the physical location/physical geography of storage of a tenant’s data upon request? | X | Google may store customer data in the following locations: [G Suite](http://www.google.com/about/datacenters/inside/locations/), [Google Cloud Platform](https://cloud.google.com/about/locations/), and for customers using Google’s Cloud CDN, the following locations apply: [https://cloud.google.com/cdn/docs/locations](https://cloud.google.com/cdn/docs/locations) |
| STA-05.4 | Can you provide the physical location/physical geography of storage of a tenant’s data in advance? | X | Google may store customer data in the following locations: [G Suite](http://www.google.com/about/datacenters/inside/locations/), [Google Cloud Platform](https://cloud.google.com/about/locations/), and for customers using Google’s Cloud CDN, the following locations apply: [https://cloud.google.com/cdn/docs/locations](https://cloud.google.com/cdn/docs/locations) |
| STA-05.5 | 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. For G Suite; please see [https://support.google.com/a/answer/9223653?hl=en](https://support.google.com/a/answer/9223653?hl=en) for more information. |
| STA-05.6 | 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. |
| STA-05.7 | Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies? | X | [https://cloud.google.com/terms/data-processing-terms](https://cloud.google.com/terms/data-processing-terms) [https://gsuite.google.com/terms/dpa_terms.html](https://gsuite.google.com/terms/dpa_terms.html) |
| STA-05.8 | Do you provide the client with a list and copies of all subprocessing agreements and keep this updated? | X | Google maintains public subprocessor lists for review. The lists are updated when subprocessors are added, modified, or removed. [Google Cloud Platform](https://cloud.google.com/terms/subprocessors) [G Suite](http://www.google.com/intl/en/terms/subprocessors.html) |
Supply Chain Management, Transparency, and Accountability

**STA-06**
Providers shall 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.

Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?  

Google employs a vendor management process that includes contractual requirements and review of vendors to ensure adherence to Google's requirements.

**STA-07**
Policies and procedures shall be established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and current agreements (e.g., SLA) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.

Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and current agreements (e.g., SLA) between providers and customers (tenants) across the relevant supply chain (upstream/downstream)?

Google maintains a dashboard for service availability information and service issues:
- https://status.cloud.google.com/
- https://www.google.com/appstatus/
Service Level Agreements may be found at:
- https://cloud.google.com/terms

**STA-08**
Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends.

Do you review all service level agreements at least annually?

Google reviews its Service Level Agreements periodically. Current Google Cloud Service Level Agreements can be found here: https://cloud.google.com/terms

Do you assure reasonable information security across your information supply chain by performing an annual review?  

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.

**STA-09**

Google maintains a Data Security Policy that governs conflict of interests.
Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?

Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?

Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?

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

Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components 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 security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?

Google's threat detection systems are constantly updated based on attack signatures encountered.

...
TVM-03.1 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 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? X Google Cloud does not rely on mobile code.

TVM-03.2 Is all unauthorized mobile code prevented from executing? X Google Cloud does not rely on mobile code.