CAIQv3.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

The information described in this paper is detailed as of the time of authorship. The information in this document does not amend or in any way alter Google's security obligations as part of its contractual agreement with Customer. Google may discontinue or change the processes, procedures and controls described in this document at any time without notice as we regularly innovate with new features and products within Google Cloud. Google's security obligations are described in its contractual agreement with Customer which may include our Data Processing Amendment and/or Data Processing and Security Terms if opted-in by Customer.

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicab	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			Google uses a continuous build and release process informed by industry practices. The controls around code release are included in the scope of our 3rd party attestations.
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			Google follows a structured code development and release process that includes considerations for security defects. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production monitoring based on real-time threats.
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	X			Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?			X	Google does not rely on software suppliers for critical services provided to customers. All critical Google products are developed by Google and follow a mature software development process.
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			Customers must agree to Google's Terms of Service and Acceptable Use Policy prior to using Google Cloud. Please see: https://cloud.google.com/terms/ for current terms relating to Google Cloud Platform and G Suite products.
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	X			The customer must identify the appropriate trust levels for access to Google Cloud and set sharing permissions accordingly. Customers are responsible for managing these types of features in their applications in Google's cloud environment.
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Does your data management policies and procedures require audits to verify data input and output integrity routines?	X			Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access.
		AIS-03.2		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?	X			The intent of this control does not apply to Google Cloud Platform. However, Google conducts integrity checks on data written to its storage systems to ensure availability and replication.

Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture satisfies industry standards such as PCI-DSS, NIST 800-53, AICPA Trust Services Criteria (SOC2), and ISO/IEC 27001 security objectives.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	X			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-01.2		Does your audit program take into account effectiveness of implementation of security operations?	X			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 and security operations against recognized standards such as PCI-DSS, NIST 800-53, AICPA Trust Services Criteria (SOC2), and ISO/IEC 27001 security objectives.
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			Google makes its SOC2, ISO/IEC 27001 and similar third-party audit or certification reports available to customers.
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google conducts rigorous internal continuous testing of our network perimeter 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		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Google conducts rigorous internal continuous testing of our application surface through various types of penetration test exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers.
		AAC-02.4		Do you conduct internal audits at least annually?	X			Google maintains an internal audit program consistent with industry best practices and regulatory requirements.
		AAC-02.5		Do you conduct independent audits at least annually?	X			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-02.6		Are the results of the penetration tests available to tenants at their request?		X		Google's Security Policy prohibits sharing this information but customers may conduct their own testing of our products and services.
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	X			Google makes its SOC 2/3 report and ISO/IEC 27001, 27017, and 27018 certificate available to customers. For a full list of available certificates and compliance materials, please refer to: https://cloud.google.com/security/compliance

Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			Customer data is logically segregated by domain to allow data to be produced for a single tenant. However, it is the responsibility of the customer to deal with legal requests. Google will provide customers with assistance with these requests, if necessary.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			Google implements a business continuity plan for our Services, reviews and tests it at least annually and ensures it remains current with industry standards. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide https://cloud.google.com/solutions/dr-scenarios-planning-guide
		BCR-01.2		Do you have more than one provider for each service you depend on?	X			Google maintains redundancy for critical services such as telecommunication links.
		BCR-01.3		Do you provide a disaster recovery capability?	X			Google automatically replicates to and serves data from multiple data centers to provide seamless access to end-users should a datacenter not be available.
		BCR-01.4		Do you monitor service continuity with upstream providers in the event of provider failure?	X			Google automatically replicates to and serves data from multiple data centers to provide seamless access to end-users should a datacenter not be available.
		BCR-01.5		Do you provide access to operational redundancy reports, including the services you rely on?		X		Google automatically replicates to and serves data from multiple data centers to provide seamless access to end-users should a datacenter not be available.
		BCR-01.6		Do you provide a tenant-triggered failover option?	X			Google Cloud Platform provides managed load balancing and failover capability to customers. https://cloud.google.com/compute/docs/load-balancing/
		BCR-01.7		Do you share your business continuity and redundancy plans with your tenants?		X		The detailed business continuity and redundancy plans are internal to Google. However, the existence and operating effectiveness of the same, is verified as part of our SOC 2/3 audit reports.
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Google performs annual testing of its business continuity plans to simulate disaster scenarios that model catastrophic events that may disrupt Google operations.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	X			Google adheres to ISO/IEC 27001/17/18, SOC 1/2/3, PCI DSS, and several other global and regional standards and frameworks, for securing,monitoring, maintaining and testing of datacenter utilities services and environmental conditions. Refer to the Google Security White Paper for further details: https://cloud.google.com/security/overview/whitepaper#environmental_impact
		BCR-03.2		Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X			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)s in case of adverse environmental conditions.

Business Continuity Management & Operational Resilience Documentation	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.
Business Continuity Management & Operational Resilience *Environmental Risks*	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, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	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=yfF3pOzdmIE **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 https://www.google.com/about/datacenters/inside/data-security/index.html
Business Continuity Management & Operational Resilience *Equipment Location*	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.
Business Continuity Management & Operational Resilience *Equipment Maintenance*	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 https://www.google.com/about/datacenters/inside/data-security/index.html
		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.

Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	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.	Are 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.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	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 • Understand threats to critical products and services • 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 disruption to your organization (i.e. 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 27001/27017/27108, PCI-DSS, SOC 1/2/3 controls) and frameworks to determine the impact of disruptions.
		BCR-09.2		Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			Google routinely performs impact analysis for possible disruptions to cloud services and performs post-mortems to understand the root cause, and mitigate future disruptions.
Business Continuity Management & Operational Resilience *Policy*	BCR-10	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.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	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 retain control and ownership over their content. Customers are responsible for managing their data retention policies. Customers may leverage the features of our storage services. Please see product documentation for specifics.
		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. As 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.

		BCR-11.4		If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Essential hardware in Google data centers are hot swappable.
		BCR-11.5		If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?	X			GCE (Google Compute Engine) provides the ability to perform full or incremental snapshots (backups) of the entire hard disk that can be restored later.
		BCR-11.6		Does your cloud solution include software/provider independent restore and recovery capabilities?	X			GCE VM image exports/imports are OS/software independent.
		BCR-11.7		Do you test your backup or redundancy mechanisms at least annually?	X			Google embeds redundancy as part of its architecture and failure is expected and corrected continuously. Google annually tests its disaster recovery program which simulates catastrophic events impacting engineering operations.
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	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-authorized by the organization's business leadership or other accountable business role or function	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			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.
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?	X			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.
		CCC-02.2		Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?	X			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.
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			Google maintains policy and procedures to ensure consideration of security, quality and availability throughout the SDLC (Software Development Lifecycle).
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X			Google maintains a dashboard for service availability information and service issues: https://status.cloud.google.com/ https://www.google.com/appsstatus Google maintains internal bug tracking of known product defects. Each bug is assigned a priority and severity rating based on the number of customers impacted and the level of potential exposure of customer data. Bugs are actioned based on ratings and remediation actions are captured in the bug tickets.
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			If a legitimate vulnerability requiring remediation has been identified by Google, it is logged, prioritized according to severity, and assigned an owner. Google tracks such issues and follows up frequently until they can verify that they have been remediated. We also have a Vulnerability Rewards Program to solicit external reports for our services. Please see: http://www.google.com/about/appsecurity/reward-program/
		CCC-03.4		Do you have controls in place to ensure that standards of quality are being met for all software development?	X			Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

		CCC-03.5		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 policies and onsite inspections, as needed, to confirm compliance.
		CCC-03.6		Are 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 makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
Change Control & Configuration Management *Outsourced Development*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	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.
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	X			Google enables customers to 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.
		CCC-05.2		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 approvals from relevant stakeholders before being released into production. Google maintains policy and procedures 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.
		CCC-05.3		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 has a robust change management process that is documented and requires approvals from relevant stakeholders before being released into production. Google maintains policy and procedures 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.
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	X			Google Cloud Compute resources support tagging. Customers assign tags to help easily apply networking or firewall settings. Tags are used by networks and firewalls to identify which instances that certain firewall rules apply to. For example, if there are several instances that perform the same task, such as serving a large website, you can tag these instances with a shared word or term and then use that tag to give HTTP access to those instances. Tags are also reflected in the metadata server, so you can use them for applications running on your instances. https://cloud.google.com/compute/docs/label-or-tag-resources
		DSI-01.2		Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X	Google tags physical hardware. Components are inventoried for easy identification and tracking within Google facilities. Other hardware characteristics, such as MAC are used for identification.
Data Security & Information Lifecycle Management	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual)	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X			Netflow policies are enforced through switch and router based ACLs. Network traffic dashboard and automated inventory tools provide real-time information on traffic flow enforcement.

Data Inventory / Flows		DSI-02.2	within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	Can you ensure that data does not migrate beyond a defined geographical residency?	X			Data stored at rest can be configured in specific products to stay in a geographic region. This is determined at time of service set up and in covered by the service specific terms: https://cloud.google.com/terms/service-terms
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			Google supports the use of open encryption methodologies. Google forces TLS for all authentication traffic. Customer data is encrypted when on Google's internal networks, in transport and at rest.
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			Google uses encryption when customer data traverses public networks. Encryption may be open-source based or proprietary.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?	X			Google maintains policies and procedures on data access and labeling.
		DSI-04.2		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	X			Customers can apply their own data-labeling standard to information stored in Google Cloud.
		DSI-04.3		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	This control is not applicable to Google Cloud. This falls under customer responsibility. Customers can apply their own data-labeling standard to information stored in Google Cloud. Customers may leverage Google's AI Platform Data Labeling Service to do so https://cloud.google.com/ai-platform/data-labeling/docs
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			Google has established procedures and technical controls to help ensure production data remains in the secure boundary of the production network.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	X			Google's terms of service address data ownership and its internal data security policies govern data stewardship.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	X			Google's process for data deletion upon termination is described in our DPST and DPA. https://cloud.google.com/terms/
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			Google's process for data deletion upon termination is described in our DPST and DPA.
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	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	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			Google maintains assets inventories and assigns ownership for managing its critical resources

		DCS-01.2	of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			Google maintains asset inventories and assigns ownership for managing its critical resources.
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system that are linked to a system alarm. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on an individual' s job responsibilities. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to help cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week.
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Do you have a capability to use system geographic location as an authentication factor?	X			Google allows domain administrators to configure alerts for potential suspicious logins. Geographic location is one factor that could indicate a suspicious login.
		DCS-03.2		Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			Google uses certificates and ACLs to achieve authentication integrity.
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			Google has strict policies and procedures for the offsite storage of encrypted backup tapes and decommissioned hardware. Software and other data is not relocated or transferred offsite.
Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with your asset management policies and procedures?		X		Google has strict policies and procedures to govern the management of the equipment lifecycle within its production data centers. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorized by appropriate operations manager before release. For more information, please see: https://cloud.google.com/security/deletion
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			Google maintains a physical security policy that describes the requirements for maintaining a safe and secure work environment.
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			Google trains its employees and contractors annually as per security policies. Third-parties agree to observe Google's security policies as part of their contract.
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			A combination of CCTV cameras, ID cards, retina scans, mantraps, and gate checkpoints are used to monitor ingress and egress at the various physical security zones in a Data Center.

Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system that are linked to a system alarm. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on an individual' s job responsibilities. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to help cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week.
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors, and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request (which is followed by proper approval process) electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved. All visitors are badged using a centralized controlled and monitored system. Google requires all visitors to sign a NDA and sign a visitor log prior to entry, and must be escorted at all times.
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	X			Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?	X			Google provides capabilities to encrypt data by tenant for a subset of products. https://cloud.google.com/security/encryption-at-rest/
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	X			Google has capabilities to manage encryption keys on behalf of tenants.
		EKM-02.3		Do you maintain key management procedures?	X			Google maintains documentation on its key management process.
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		X		Google uses a combination of open source and proprietary code to develop its encryption solutions.
Encryption & Key Management	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			Google maintains encryption at rest for customer data.

Encryption		EKM-03.2	processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			Google employs several security measures to help ensure the authenticity, integrity, and privacy of data in transit.
		EKM-03.3		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			Google maintains documentation for the use of its internal proprietary key management service.
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			Google uses a combination of open source and proprietary encryption formats and algorithms validated by Google security engineers.
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			Google maintains its own encryption keys.
		EKM-04.3		Do you store encryption keys in the cloud?	X			Google stores its keys in its own production environment.
		EKM-04.4		Do you have separate key management and key usage duties?	X			Google's key management operates as a service for engineering teams to use in their application code.
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			Google maintains security configurations for its machines and networking devices. The configurations are maintained and serve as master copies for comparison against production instances. Deviations are identified and corrected.
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			Google has automated mechanisms to detect deviations from the desired security configuration of its infrastructure.
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			Google takes into account regulatory, legal, and statutory requirements applicable to data, including data retention, classification and protection, in its risk assessments. Google has demonstrated adherence to this control by way of ISO/IEC 27001/27018 certifications, as well as the annual external third party audits conducted for SOC 2/3 compliance. Google provides customers (under NDA) SOC 2 report that demonstrates compliance with these controls.
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X			Google performs risk assessments as required to support its ISMS.
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			Management is responsible for ensuring direct reports complete all required trainings and affidavits. Sanctions are put in place for Googlers who do not complete required training within the required time period.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Google also maintains an internal ISMS and evidence of its effectiveness is provided via ISO/IEC 27001 certification.

		GRM-04.2	unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management	Do you review your Information Security Management Program (ISMP) at least once a year?	X			Google reviews its ISMS documentation annually as part of its required due diligence.
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			Google executive management reviews and approves all information security policies and set applicable commitment and direction to achieve the agreed upon Information Security goals.
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			Information Security policies and procedures are communicated to all internal employees that must undergo and attest to yearly training.
		GRM-06.2		Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	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 ISMS, roles and responsibilities are documented and authorized by leadership.
		GRM-06.3		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-06.4		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	X			Google has mapped its security controls to the requirements of the AICPA Trust Services Criteria (SOC2), NIST 800-53, and ISO/IEC 27002.
		GRM-06.5		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	X			Google maintains a public website that details all current compliance, regulatory, and privacy standards Google either complies or aligns with.
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Google maintains a personnel policy that includes disciplinary procedures.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			Google makes its internal policies available to all personnel. Communication of policies occurs via required training, and through ongoing e-mail and internal communication. Employees must review and confirm understanding of key security and privacy policies (including what actions are taken if an employee is in violation of said policy) at least annually, and records of certification are retained to ensure compliance. Google's code of conduct is available publicly at our investor website. https://abc.xyz/investor/other/code-of-conduct/
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			Documentation updates to policies, standards, and controls identified through the risk assessment process will be triaged and addressed by Google's Security Policy team.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			Google notifies tenants of material changes to contractually committed terms. Google does not notify tenants of changes to internal policies.

		GRM-09.2	a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			Google reviews its security and privacy policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risk and issue new or amend existing policies or guidelines, as needed.
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			Google's risk assessments are conducted annually and are aligned with the enterprise risk framework. The risk assessment uses both qualitative and quantitative methods to determine likelihood and impact of events.
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X			Google's risk assessment considers inherent and residual risk factors as part of its review process.
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?	X			Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification.
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	X			Google has documented its risk management procedures as part of its ISMS that underlies our ISO/IEC 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs.
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			Google has a well defined exit 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.
		HRS-01.2		Do you have asset return procedures outlining how assets should be returned within an established period?	X			Google has a well defined exit process including equipment return procedures for terminated employees.
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			Google employees must attest to the Code of Conduct, sign a NDA and undergo yearly Information Security Policy and Training with an ackowledgement to complete, prior to getting access to Google systems. Google undergoes periodic compliance audits to validate that employees understand and follow the established policies. Refer to SOC report for details.
		HRS-03.2		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?	X			Google employees must attest to the Code of Conduct, sign a NDA and undergo yearly Information Security Policy and Training with an ackowledgement to complete, prior to getting access to Google systems. Google undergoes periodic compliance audits to validate that employees understand and follow the established policies.
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			Google maintains personnel and data access policies that govern the administration of access controls including transfers and terminations.
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			Google's personnel policies include requirements for the timely removal of access and return to Google issued assets.

Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			Google maintains a mobile device policy that details our requirements for mobile device use at Google. Customer data is not permitted on mobile devices.
Human Resources *Non-Disclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			Google reviews NDA and confidentiality documents as needed.
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			Google's Terms of Service outline the responsibilities of Google and customers.
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			Google has a Code of Conduct and Information Security Policy that governs the usage of devices at Google.
		HRS-08.2		Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	X			Google has a well defined Mobile Device Management Policy that governs and defines the allowances and conditions for the use of corporate services. BYOD 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.
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually.
		HRS-09.2		Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			Google provides role-specific privacy and security training. The training is administered online and completion is tracked. Privacy and security training are required annually.
		HRS-09.3		Do you document employee acknowledgment of training they have completed?	X			Personnel are required to acknowledge the training they have completed.
		HRS-09.4		Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			Completion of the training is required by our personnel policies.
		HRS-09.5		Are personnel trained and provided with awareness programs at least once a year?	X			Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually.
		HRS-09.6		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			Customers are responsible for ensuring proper education and identifying legal responsibilities of their staff as it relates to customer applications and data. Google personnel are trained on the Data Security policy including procedures for handling customer data.
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			Google maintains a security awareness program for its personnel. Customers are responsible for training their users.
		HRS-10.2		Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			Google maintains a security awareness program for its personnel. Customers are responsible for training their users.
		HRS-10.3		Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			Google maintains a security awareness program for its personnel. Customers are responsible for training their users.

Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			Workstations, laptops, and mobile devices are configured such that they lockout after a pre-defined period of time, as per policy.
		HRS-11.2		Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			Google has a well established security policy that requires all personnel to not leave sensitive materials unattended.
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools.
		IAM-01.2		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 our production environment.
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third-party (e.g., provider and/or other customer (tenant)	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment.
		IAM-02.2		Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			Google restricts access based on need-to-know and job function in accordance with applicable legal and compliance requirements. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls.
		IAM-02.3		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.
		IAM-02.4		Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			Google restricts access to information by determining if the access authorization assigned to the sharing partner matches the access restrictions on the information. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls.
		IAM-02.5		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. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls.
		IAM-02.6		Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	X			Google maintains policies and procedures that enforce data access permissions. Two factor authentication is required for all employee access to all company and customer resources. Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls.

		IAM-02.7	any third party (e.g., provider and/or other customer (tenant) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements **Requirements in bullet points 4 to 7 are covered in IAM-12 questions.*	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	X			Google logs all changes in user permissions with the date and time of such changes.
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			Google restricts access based on need-to-know and job function. Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls.
Identity & Access Management *Policies and Procedures*	IAM-04	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.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			Google maintains a central identity and authorization management system.
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			Google maintains a central identity and authorization management system.
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			Google provides (under NDA) customers with a SOC 2 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Google restricts access based on need-to-know and job function. Google maintains automated log collection and analysis tools.
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to	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.

		IAM-07.2	minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	X			Google restricts access based on need-to-know and job function.
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			Google restricts access based on need-to-know and job function.
		IAM-08.2		Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X			Google restricts access based on need-to-know and job function.
		IAM-08.3		Do you limit identities' replication only to users explicitly defined as business necessary?	X			Google restricts access based on need-to-know and job function.
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			Customers are responsible for configuring the access by their users to the service. For Google personnel, authorization is required prior to access being granted.
		IAM-09.2		Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?			X	Customers are responsible for configuring the access by their users to the service. For Google personnel, authorization is required prior to access being granted.
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			Google requires access reviews at least semi-annually for critical access groups.
		IAM-10.2		Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			As a part of Google's 3rd party attestation reports, annual external audits for SOC 2 compliance is conducted. Google provides customers (under NDA) SOC 2 report that demonstrates compliance with these controls.
		IAM-10.3		Do you ensure that remediation actions for access violations follow user access policies?	X			Google logs all changes in user permissions. Google revokes access when no longer required.
		IAM-10.4		Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?		X		Google notifies customers of security incidents that impact their data and will work with the customer in good faith to address any known breach of Google's security obligations.
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically reviews access lists and removes access that is no longer required. All account actions are recorded.
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically reviews access lists and removes access that is no longer required. All account actions are recorded.
Identity & Access Management	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			Google supports integration with a customer's SSO solution.

User ID Credentials		IAM-12.2	access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you use open standards to delegate authentication capabilities to your tenants?	X			Google support 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 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, giving full control and visibility 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 processes. 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.
		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 3rd 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 Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			ACLs for production tools are appropriately scoped to perform job function.

Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			Google has implemented network and host based tools to detect and respond to potential security incidents. Google maintains automated log collection and analysis tools to support investigations.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			Google restricts physical and logical access to audit logs.
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?	X			Google has mapped its security controls to the requirements of the AICPA Trust Services Criteria (SOC2), NIST 800-53, and ISO/IEC 27002.
		IVS-01.4		Are audit logs centrally stored and retained?	X			Google maintains an automated log collection and analysis tool to review and analyse log events.
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			Google maintains an automated log collection and analysis tool to review and analyse log events.
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			Google machine configuration changes are continuously monitored when online.
		IVS-02.2		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			Google does not use a virtual infrastructure. Google maintains configuration management tools to detect and correct deviations from its security baselines and collects and secures audit records.
		IVS-02.3		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	X			Cloud Security Command Center provides visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems. Please see https://cloud.google.com/security-command-center/docs/ for more information. In addition, Shielded VM's enable live measurement, monitoring, and alerting for any changes of the full stack. https://cloud.google.com/shielded-vm/ https://cloud.google.com/security/shielded-cloud/shielded-vm
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			Google uses a synchronized time-service protocol to ensure all systems have a common time reference. Google makes their NTP protocol public as well for use by customers. https://developers.google.com/time/
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?			X	Google maintains an effective resource economy with internal Service Level Agreements between engineering teams that provide for capacity planning and provisioning decisions.
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			Google has implemented efficient memory management techniques in the virtual machine system.
		IVS-04.3		Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			Google maintains an effective resource economy with internal Service Level Agreements between engineering teams that provide for capacity planning and provisioning decisions.
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			Google's engineering teams monitor the performance and health of infrastructure components against their internal Service Level Agreement commitments that in turn support business and regulatory requirements.

Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			Google performs fuzz testing, penetration testing, and vulnerability scanning to detect, mitigate, and resolve security issues.
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	X			Google provides solution papers and reference docs for various architectures and intended solutions.
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?			X	Google maintains network diagrams for internal purposes, that are dynamic and updated regularly.
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			The security state of network devices is monitored continuously.
		IVS-06.4		Are all firewall access control lists documented with business justification?	X			Network ACLs are documented within configuration files with comments on purpose, as appropriate.
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			Google builds its own machines and deploys custom operating system images that only permit the necessary ports, protocols, and services.
Infrastructure & Virtualization Security *Production / Non-Production Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Customers can provision separate domains or organizations within a domain for testing purposes.
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	X			Google provides solution papers and reference docs for development and test environments. https://cloud.google.com/solutions/devtest/
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	X			Google segregates its production environment from its corporate environment.
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			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.
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			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.
		IVS-09.3		Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	X			Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customer data is logically segregated by domain to allow data to be produced for a single tenant.
		IVS-09.4		Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			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.
		IVS-09.5		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			Customers can use organizational structures with their environment to help manage segregation of sensitive data.

Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. Please see https://cloud.google.com/security/encryption-in-transit/ for more information.
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			Google's production network is separated from other networks.
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor 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, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			All access to production systems is based on least privilege, requires two-factor authentication, and is logged.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	Google does not permit wireless access in the production environment. Google has established policies and procedures to manage its corporate wireless network perimeter.
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X	Google does not permit wireless access points in its production environment. Google has established strong encryption and authentication to its corporate wireless network.
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	X			Google does not permit wireless access points in its production environment and periodically scans for rogue devices.
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	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.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?			X	Google maintains a purpose built tool to dynamically identify changes to the network in real-time.
		IVS-13.2		Do you implement technical measures and 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?	X			Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves: 1. Tightly controlling the size and make-up of Google's attack surface through preventative measures; 2. Employing intelligent detection controls at data entry points; and 3. Employing technologies that automatically remedy certain dangerous situations. Please review https://cloud.google.com/security/infrastructure/design/ regarding defense-in-depth techniques deployed across our infrastructure.
Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Google publishes information on its Google Cloud Platform and G Suite APIs. https://cloud.google.com/docs/ https://developers.google.com/google-apps/
Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			Customers do not need Google's assistance to port their data. Customers can export their data from G Suite using Google Takeout. https://takeout.google.com/settings/takeout Customers can export their Google Cloud Platform data in a number of industry standard formats.
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X			Customers should evaluate the APIs Google provides for suitability in third-party applications. Google makes detailed information available on the use and function of its APIs. Terms of Service for APIs are located on their respective pages.

		IPY-03.2	for application development and information exchange, usage, and integrity persistence.	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	X			Customers can export/import an entire VM image in the form of a .tar archive.
		IPY-03.3		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			Service Level Agreements are covered by the service specific terms: https://cloud.google.com/terms/
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			Network traffic is encrypted using industry standard protocols.
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			Google provides documentation regarding how customers may port data. Our GDPR resource site provides an entry point for information regarding portability and interoperability of data. https://cloud.google.com/security/gdpr/
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			Google supports most virtual disk file formats, including VMDK, VHD and RAW.
		IPY-05.2		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	X			Customers can export/import an entire VM image in the form of a .tar archive.
		IPY-05.3		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	X			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/
Mobile Security *Anti-Malware*	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	X			Google provides security awareness training to all employees and includes references to our security policies, including our mobile device policies. Training also includes how to protect data when using mobile devices in public and identifying potentially malicious actors.
Mobile Security *Application Stores*	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	X			Google's mobile device policy does not permit the use of third-party application stores.
Mobile Security *Approved Applications*	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	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 a mobile device?	X			The Google Device Policy restricts the user and device behavior on mobile devices including application installation. For advanced use, a work profile is required which includes a restricted apps store.
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	X			The Google Device Policy restricts the user and device behavior on mobile devices including application installation. For advanced use, a work profile is required which includes a restricted apps store.
Mobile Security *Awareness and Training*	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	X			Google provides security awareness training to all employees that includes references to our security policies, including our mobile device policies. Training also includes how to protect data when using mobile devices in public.
Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	X			Google only permits the storage of Google sensitive information in approved systems.
Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?	X			Mobile operability is is part of our standard software engineering development lifecycle.
Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	X			Google maintains a mobile policy and provides detailed instructions to personnel that wish to provision access to Google services on their mobile device. The policy includes eligibility requirements and security policy requirements.
Mobile Security *Device Inventory*	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e.,	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?	X			All devices must register through the Google Device Policy Manager unless browser-only access is used.
Mobile Security *Device Management*	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	X			Google's Device Policy Manager enforces Google's mobile policy except when access is solely to Apps services and through a browser.

Mobile Security *Encryption*	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	X			Mobile devices with access to corporate resources other than Apps services require encryption.
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	X			Google's mobile policy does not permit jailbreaking or rooting on devices linked to a Google corporate account.
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	X			Google's Device Policy Manager may not install on a device that does not conform to the required security specifications. The Device Policy Manager is required in order to access corporate sources using mobile applications.
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	X			Google's mobile policy states that all security policies apply in a mobile environment.
		MOS-13.2		Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?	X			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.
Mobile Security *Lockout Screen*	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	X			Google's Device Policy Manager requires personnel to set an automatic lockout screen.
Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?	X			Google's Device Policy Manager requires personnel to keep devices up to date with patches and requires a minimum O/S level.
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	X			Google's Device Policy Manager enforces password policies.
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?	X			Google's Device Policy Manager enforces password policies.
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	X			Devices are assigned minimum password requirements that cannot be circumvented by the user.
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	Google does not permit access to production data in mobile devices.
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	X			Google's mobile device policy does not permit the use of unapproved application stores.
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	X			Google requires all mobile devices (including personally owned devices) to conform to corporate device management policies that apply restrictive controls to reduce the risk of malware-based attacks.
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	X			Google requires all mobile devices (including personally owned devices) to conform to device management policies, including remote wipe capabilities.
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	X			Google requires remote wipe capabilities for all mobile devices managed by Google.
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	X			Google's mobile policy requires the installation of all updates and sets minimum O/S requirements.
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	X			Google's mobile policy requires the installation of all updates and sets minimum O/S requirements.
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	X			Google's mobile policy defines which corporate resources can be accessed with a mobile device and the level of protections associated with such access.
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	X			Google's mobile policy defines which roles (profiles) can access corporate resources.

Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	X			Google maintains incident response procedures to help ensure prompt notification and investigation of incidents.
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?	X			Google has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority.
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			Google's Terms of Service cover roles and responsibilities. https://cloud.google.com/terms/
		SEF-02.4		Have you tested your security incident response plans in the last year?	X			Google performs annual testing of its emergency response processes.
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			Google has a well established a privacy and information security training program that informs personnel of their responsibility to report security events in a timely manner.
		SEF-03.2		Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			Google has a well defined and 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. Additionally, Google communicates outage information through its status dashboards: For Cloud Platform: https://status.cloud.google.com/ For G Suite: https://www.google.com/appsstatus#hl=en&v=status Google's end-to-end data incident response process is described in this whitepaper https://cloud.google.com/security/incident-response
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			Google can support properly formed requests for specific tenant data when requested by law enforcement.
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			Google can support properly formed requests for specific tenant data when requested by law enforcement.
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			Google Cloud Platform customers may implement this feature with external products or by using the "Bucket Lock" features available in Cloud Storage. G Suite customers may purchase Vault for their domain, which allows an organization to create retention/litigation holds without impacting other tenants.
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			Google can support properly formed requests for specific tenant data when requested by law enforcement.

Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			Google reviews and analyzes security incidents to determine impact, cause, and opportunities for corrective action.
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?		X		The amount of security incident data is currently statistically insignificantly small. Should the amount of data increase, Google will consider sharing this statistical information.
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?			X	This falls under customer responsbility as they retain control and owenrship over the quality of their data and potential quality errors that may arise through their usage of Google Cloud.
		STA-01.2		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?	X			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.
Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			Individual customers get notified should an incident impact their data. Google communicates outage information through our status dashboards: For Cloud Platform: https://status.cloud.google.com/ For G Suite: https://www.google.com/appsstatus
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Google collects capacity and use data on its infrastructure as needed to inform capacity planning and internal Service Level Agreement performance.
		STA-03.2		Do you provide tenants with capacity planning and use reports?	X			Google Cloud Platform allows customers to monitor the consumption of their services. G Suite is a pay per seat product where capacity management is the responsibility of Google.
Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			Google maintains an internal program to assess ongoing conformance with relevant policies, processes, and metrics.
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations)	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			Google's agreements with subprocessors are subject to applicable laws and regulations.
		STA-05.2		Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			Google has a well defined vendor management policy and process to select and monitor third party providers. Google conducts ongoing audits of subprocessors for compliance.
		STA-05.3		Does legal counsel review all third-party agreements?	X			Third party agreements go through multiple levels of review, including legal review by appropriate counsel.
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			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-05.5	compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	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.
		STA-05.6		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			Customers can choose data location in the US and Europe when configuring some of their Google Cloud Platform services. If these selections are made around choice of data location, this is backed by the service specific terms within Google's Terms of Service.
		STA-05.7		Can you provide the physical location/geography of storage of a tenant's data upon request?	X			Google may store customer data in the following locations: G Suite: http://www.google.com/about/datacenters/inside/locations/ Google Cloud Platform: https://cloud.google.com/about/locations/ For customers using Google's Cloud CDN, the following locations apply: https://cloud.google.com/cdn/docs/locations
		STA-05.8		Can you provide the physical location/geography of storage of a tenant's data in advance?	X			Google may store customer data in the following locations: G Suite: http://www.google.com/about/datacenters/inside/locations/ Google Cloud Platform: https://cloud.google.com/about/locations/ For customers using Google's Cloud CDN, the following locations apply: https://cloud.google.com/cdn/docs/locations
		STA-05.9		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.
		STA-05.10		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-05.11		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?			X	Our data processing terms detail how we process tenant data.
		STA-05.12		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: https://gsuite.google.com/intl/en/terms/subprocessors.html

Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	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?	X			Google employs a vendor management process that includes contractual requirements and review of vendors to ensure adherence to Google's requirements.
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) 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 relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			The customer terms of services are updated as needed.
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	X			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-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			Internal reviews of supplier contracts may consider conflicts of interest, as applicable, based on the nature of the contract.
		STA-07.4		Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			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-07.5		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X			Google provides customers with uptime availability metrics and industry standard audit reports and certifications.
		STA-07.6		Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			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-07.7		Do your data management policies and procedures address tenant and service level conflicts of interests?	X			Google maintains a Data Security Policy that governs conflict of interests.
		STA-07.8		Do you review all service level agreements at least annually?	X			Google reviews its Service Level Agreements periodically. Current Google Cloud Service Level Agreements can be found here: https://cloud.google.com/terms
Supply Chain Management, Transparency, and Accountability *Third Party*	STA-08	STA-08.1	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 on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			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-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			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.

Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	X			Google conducts annual reviews and audits of its subprocessors to validate adherence with Google's security requirements to ensure they provide a level of privacy and security appropriate to their access to data and the scope of the services. Google engages with third party service providers, which can be found in the Terms of Service. Refer https://cloud.google.com/terms for more information. Refer https://cloud.google.com/terms/data-processing-terms#11-subprocessors for more information.
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			Google retains a 3rd party to conduct vulnerability scans and periodic penetration tests.
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and 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?	X			Google maintains an internal set of controls to detect and prevent malware on its own systems. Malware detection is included in our G Suite service. Gmail scans for malware in email, attachments, and Drive scans files prior to upload.
		TVM-01.2		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?	X			Google's threat detection systems are constantly updated based on attack signatures encountered.
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			Google performs periodic network vulnerability scans using commercial and proprietary tools.
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			Google performs periodic application-layer vulnerability scans using commercial and proprietary tools.
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			Google performs periodic local operating system-layer scans and checks using commercial and proprietary tools.
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?		X		Google does not make internal vulnerability scan results available to customers. Customers may perform their own scans on their own projects or public address space at any time.
		TVM-02.5		Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			Google operates a homogeneous machine environment with custom software to minimize exposure to vulnerabilities in commercial products and to allow rapid patching if needed.
		TVM-02.6		Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?			X	This does not apply to Google as customer data is not used as part of Google Cloud services. Customers are responsible for vulnerability management within their accounts and hosted solutions, while Google safeguards the overall security of Google Cloud services. Products such as Cloud Security Scanner https://cloud.google.com/security-scanner can be used by customers for automated vulnerability scanning, and Cloud Armor https://cloud.google.com/armor/ can be used to protect their applications against Denial of service and Web attacks. Customer notification responsibilities are mutually agreed per contracts. Refer to our terms of service here https://cloud.google.com/terms Additionally, refer to our security whitepaper https://cloud.google.com/security/overview/whitepaper#vulnerability_management

Threat and Vulnerability Management *Mobile Code*	TVM-03	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.