Spring-2024 Google Cloud Services Statement of Applicability	
Rationale Definitions	
Risk	Control is selected specifically to address an identified risk.
Contractual	Control is selected to fulfill a specific or general contractual obligation.
Regulatory	Control is selected to fulfill a specific or general regulatory obligation.
Culture	Control is selected to fulfill company policy, guidelines, or common practice based on Google's mission and values.

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27017:2015	[ISO 27017] 5.1.1-P Policies for information security	27017 - Provider Implementation Guidance: The cloud service provider should augment its information security policy to address the provision and use of its cloud services, taking the following into account: □ the baseline information security requirements applicable to the design and implementation of the cloud service; □ risks from authorized insiders; □ multi-tenancy and cloud service customer isolation (including virtualization); □ access to cloud service customer assets by staff of the cloud service provider; □ access control procedures, e.g., strong authentication for administrative access to cloud services; □ communications to cloud service customers during change management; □ virtualization security; □ access to and protection of cloud service customer data; □ lifecycle management of cloud service customer accounts; □ communication of breaches and information sharing guidelines to aid investigations and forensics.	Code of Conduct	The organization has established a code of conduct that is reviewed and updated as needed.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 5.1.1-P Policies for information security	27017 - Provider Implementation Guidance: The cloud service provider should augment its information security policy to address the provision and use of its cloud services, taking the following into account: □ the baseline information security requirements applicable to the design and implementation of the cloud service; □ risks from authorized insiders; □ multi-tenancy and cloud service customer isolation (including virtualization); □ access to cloud service customer assets by staff of the cloud service provider; □ access control procedures, e.g., strong authentication for administrative access to cloud services; □ communications to cloud service customers during change management; □ virtualization security; □ access to and protection of cloud service customer data; □ lifecycle management of cloud service customer accounts; □ communication of breaches and information sharing guidelines to aid investigations and forensics.	Policies for information security	The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 5.1.1-P Policies for information security	27017 - Provider Implementation Guidance: The cloud service provider should augment its information security policy to address the provision and use of its cloud services, taking the following into account: □ the baseline information security requirements applicable to the design and implementation of the cloud service; □ risks from authorized insiders; □ multi-tenancy and cloud service customer isolation (including virtualization); □ access to cloud service customer assets by staff of the cloud service provider; □ access control procedures, e.g., strong authentication for administrative access to cloud services; □ communications to cloud service customers during change management; □ virtualization security; □ access to and protection of cloud service customer data; □ lifecycle management of cloud service customer accounts; □ communication of breaches and information sharing guidelines to aid investigations and forensics.	Equipment siting and protection	The organization has policies and guidelines that govern how to keep the organization' s physical workplaces, facilities, and property safe.	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 6.1.1-P Information security roles and responsibilities	27017 - Provider Implementation Guidance: The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.	Information security roles and responsibilities	The organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 6.1.3-P Contact with authorities	27017 - Provider Implementation Guidance: The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data.	Contact with law enforcement authorities	The organization establishes designated legal counsel and Government Affairs officials in order to maintain appropriate contacts with law enforcement authorities.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 6.1.3-P Contact with authorities	27017 - Provider Implementation Guidance: The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data.	Geographic location of customer data	The organization specifies and documents the countries and/or data center locations in which customer data might possibly be stored and transferred.	Privacy	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] 7.2.2-P Information security awareness, education and training	27017 - Provider Implementation Guidance: The cloud service provider should provide awareness, education and training for employees, and request contractors to do the same, concerning the appropriate handling of cloud service customer data and cloud service derived data. This data can contain information confidential to a cloud service customer or be subject to specific limitations, including regulatory restrictions, on access and use by the cloud service provider.	Information security and privacy awareness, education and training	The organization has established a privacy and information security training program and requires relevant personnel to complete this training annually.	Confidentiality, Integrity, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 8.1.1-P Inventory of assets	27017 - Provider Implementation Guidance: The inventory of assets of the cloud service provider should explicitly identify: □ cloud service customer data; □ cloud service derived data.	Inventory of corporate endpoint assets	The organization maintains an up-to-date, accurate client device inventory	Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 8.2.2-P Labelling of information	27017 - Provider Implementation Guidance: The cloud service provider should document and disclose any service functionality it provides allowing cloud service customers to classify and label their information and associated assets.	Data Classification	The organization has established policies and guidelines to govern data classification, labeling and security.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 9.2.1-P User registration and de-registration	27017 - Provider Implementation Guidance: To manage access to cloud services by a cloud service customer's cloud service users, the cloud service provider should provide user registration and deregistration functions, and specifications for the use of these functions to the cloud service customer.	User registration and de-registration	The organization maintains formal user registration and de-registration procedures for granting and revoking access.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 9.2.2-P User access provisioning	27017 - Provider Implementation Guidance: The cloud service provider should provide functions for managing the access rights of the cloud service customer's cloud service users, and specifications for the use of these functions.	Administrator's operational security	Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] 9.2.3-P Management of privileged access rights	27017 - Provider Implementation Guidance: The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risks. For example, the cloud service provider can provide multi-factor authentication capabilities or enable the use of third-party multi-factor authentication mechanisms.	Access to Prod & Network	Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 9.2.4-P Management of secret authentication information of users	27017 - Provider Implementation Guidance: The cloud service provider should provide information on procedures for the management of the secret authentication information of the cloud service customer, including the procedures for allocating such information and for user authentication.	Password Guidelines	The organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27017:2015	[ISO 27017] 9.4.4-P Use of privileged utility programs	27017 - Provider Implementation Guidance: The cloud service provider should identify the requirements for any utility programs used within the cloud service. The cloud service provider should ensure that any use of utility programs capable of bypassing normal operating or security procedures is strictly limited to authorized personnel, and that the use of such programs is reviewed and audited regularly.	Internal Tools Access	Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 10.1.1-P Policy on the use of cryptographic controls	27017 - Provider Implementation Guidance: The cloud service provider should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the information it processes. The cloud service provider should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.	Terms of Service - External Communication	The organization's commitments to security, availability, processing integrity, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS).	Availability, Confidentiality, Integrity, Privacy	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] 10.1.1-P Policy on the use of cryptographic controls	27017 - Provider Implementation Guidance: The cloud service provider should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the information it processes. The cloud service provider should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.	Customer communication of cryptographic protections	The organization provides customers with information regarding default encryption methods used to protect user data. Additional applications of cryptographic protections are documented and shared through public sites.	Confidentiality, Integrity	Risk, Culture, Contractual
ISO/IEC 27017:2015	[ISO 27017] 11.2.7-P Secure disposal or re-use of equipment	27017 - Provider Implementation Guidance: The cloud service provider should ensure that arrangements are made for the secure disposal or reuse of resources (e.g., equipment, data storage, files, memory) in a timely manner.	Secure disposal or reuse of equipment	The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 12.1.2-P Change management	27017 - Provider Implementation Guidance: The cloud service provider should provide the cloud service customer with information regarding changes to the cloud service that could adversely affect the cloud service. The following will help the cloud service customer determine the effect the changes can have on information security: □ categories of changes; □ planned date and time of the changes; □ technical description of the changes to the cloud service and underlying systems; □ notification of the start and the completion of the changes. When a cloud service provider offers a cloud service that depends on a peer cloud service provider, then the cloud service provider might need to inform the cloud service customer of changes caused by the peer cloud service provider.	Change management policies	The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Availability, Confidentiality, Integrity, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 12.1.3-P Capacity management	27017 - Provider Implementation Guidance: The cloud service provider should monitor the total resource capacity to prevent information security incidents caused by resource shortages.	Resource Management Guidelines	The organization makes procedures related to the management of information processing resources available. Procedures include guidance on requesting, monitoring and maintaining resources, and guidance around evaluating capacity demand.	Availability	Risk, Contractual, Culture, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 12.1.3-P Capacity management	27017 - Provider Implementation Guidance: The cloud service provider should monitor the total resource capacity to prevent information security incidents caused by resource shortages.	Capacity management	The organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 12.3.1-P Information backup	27017 - Provider Implementation Guidance: The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, as appropriate: □ scope and schedule of backups; □ backup methods and data formats, including encryption, if relevant; □ retention periods for backup data; □ procedures for verifying integrity of backup data; □ procedures and timescales involved in restoring data from backup; □ procedures to test the backup capabilities; □ storage location of backups. The cloud service provider should provide secure and segregated access to backups, such as virtual snapshots, if such service is offered to cloud service customers.	Service Redundancy	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 12.3.1-P Information backup	27017 - Provider Implementation Guidance: The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, as appropriate: □ scope and schedule of backups; □ backup methods and data formats, including encryption, if relevant; □ retention periods for backup data; □ procedures for verifying integrity of backup data; □ procedures and timescales involved in restoring data from backup; □ procedures to test the backup capabilities; □ storage location of backups. The cloud service provider should provide secure and segregated access to backups, such as virtual snapshots, if such service is offered to cloud service customers.	Shared responsibility within a cloud computing environment	The organization provides information pertaining to the shared responsibilities of both itself and the cloud service customer.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] 12.4.1-P Event logging	27017 - Provider Implementation Guidance: The cloud service provider should provide logging capabilities to the cloud service customer.	Administrator's operational security	Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] 12.4.1-P Event logging	27017 - Provider Implementation Guidance: The cloud service provider should provide logging capabilities to the cloud service customer.	Event logging	Audit logs are continuously monitored for events related to security, availability, processing integrity, and confidentiality threats. Alerts are generated for further investigation.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 12.4.4-P Clock synchronisation	27017 - Provider Implementation Guidance: The cloud service provider should provide information to the cloud service customer regarding the clock used by the cloud service provider's systems, and information about how the cloud service customer can synchronize local clocks with the cloud service clock.	Shared responsibility within a cloud computing environment	The organization provides information pertaining to the shared responsibilities of both itself and the cloud service customer.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] 12.6.1-P Management of technical vulnerabilities	27017 - Provider Implementation Guidance: The cloud service provider should make available to the cloud service customer information about the management of technical vulnerabilities that can affect the cloud services provided.	Vulnerability management program	The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 13.1.3-P Segregation in networks	27017 - Provider Implementation Guidance: The cloud service provider should enforce segregation of network access for the following cases: □ segregation between tenants in a multi-tenant environment; □ segregation between the cloud service provider's internal administration environment and the cloud service customer's cloud computing environment. Where appropriate, the cloud service provider should help the cloud service customer verify the segregation implemented by the cloud service provider.	Network Segmentation	The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/ or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 13.1.3-P Segregation in networks	27017 - Provider Implementation Guidance: The cloud service provider should enforce segregation of network access for the following cases: □ segregation between tenants in a multi-tenant environment; □ segregation between the cloud service provider's internal administration environment and the cloud service customer's cloud computing environment. Where appropriate, the cloud service provider should help the cloud service customer verify the segregation implemented by the cloud service provider.	Security of Wireless Networks	Wireless connections to Corp resources at organization's facilities are encrypted	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27017:2015	[ISO 27017] 14.1.1-P Information security requirements analysis and specification	27017 - Provider Implementation Guidance: The cloud service provider should provide information to the cloud service customers about the information security capabilities they use. This information should be informative without disclosing information that could be useful to someone with malicious intent.	Information security requirements analysis and specification	The organization has guidelines specifying the security requirements for new and existing information systems.	Integrity, Availability, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 14.2.1-P Secure development policy	27017 - Provider Implementation Guidance: The cloud service provider should provide information about its use of secure development procedures and practices to the extent compatible with its policy for disclosure.	Secure Development - Policies & Procedures	The organization has policies and guidelines governing the secure development lifecycle.	Confidentiality, Privacy, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 15.1.2-P Addressing security within supplier agreements	27017 - Provider Implementation Guidance: The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider will implement to ensure no misunderstanding between the cloud service provider and cloud service customer. The relevant information security measures that the cloud service provider will implement can vary based on the type of cloud service the cloud service customer is using.	Agreements for exchange of Information	The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 15.1.2-P Addressing security within supplier agreements	27017 - Provider Implementation Guidance: The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider will implement to ensure no misunderstanding between the cloud service provider and cloud service customer. The relevant information security measures that the cloud service provider will implement can vary based on the type of cloud service the cloud service customer is using.	Obligation to Protect User Data (Service Providers)	The organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 15.1.2-P Addressing security within supplier agreements	27017 - Provider Implementation Guidance: The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider will implement to ensure no misunderstanding between the cloud service provider and cloud service customer. The relevant information security measures that the cloud service provider will implement can vary based on the type of cloud service the cloud service customer is using.	Obligation to Protect Customer Data (Data Processors/Controllers)	The organization requires subprocessors to meet security & privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements or other data processing terms.	Availability, Confidentiality, Integrity, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 15.1.3-P Information and communication technology supply chain	27017 - Provider Implementation Guidance: If a cloud service provider uses cloud services of peer cloud service providers, the cloud service provider should ensure information security levels to its own cloud service customers are maintained or exceeded. When the cloud service provider provides cloud services based on a supply chain, the cloud service provider should provide information security objectives to suppliers, and request each of the suppliers to perform risk management activities to achieve the objectives.	Agreements for exchange of Information	The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 15.1.3-P Information and communication technology supply chain	27017 - Provider Implementation Guidance: If a cloud service provider uses cloud services of peer cloud service providers, the cloud service provider should ensure information security levels to its own cloud service customers are maintained or exceeded. When the cloud service provider provides cloud services based on a supply chain, the cloud service provider should provide information security objectives to suppliers, and request each of the suppliers to perform risk management activities to achieve the objectives.	Obligation to Protect User Data (Service Providers)	The organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 15.1.3-P Information and communication technology supply chain	27017 - Provider Implementation Guidance: If a cloud service provider uses cloud services of peer cloud service providers, the cloud service provider should ensure information security levels to its own cloud service customers are maintained or exceeded. When the cloud service provider provides cloud services based on a supply chain, the cloud service provider should provide information security objectives to suppliers, and request each of the suppliers to perform risk management activities to achieve the objectives.	Obligation to Protect Customer Data (Data Processors/Controllers)	The organization requires subprocessors to meet security & privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are enforced via the "Subprocessor Data Protection Agreement (SDPA)" addendum to contractual agreements or other data processing terms.	Availability, Confidentiality, Integrity, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 16.1.1-P Responsibilities and procedures	27017 - Provider Implementation Guidance: As a part of the service specifications, the cloud service provider should define the allocation of information security incident management responsibilities and procedures between the cloud service customer and the cloud service provider. The cloud service provider should provide the cloud service customer with documentation covering: □ the scope of information security incidents that the cloud service provider will report to the cloud service customer; □ the level of disclosure of the detection of information security incidents and the associated responses; □ the target timeframe in which notifications of informationsecurity incidents will occur; □ the procedure for the notification of information security incidents; □ contact information for the handling of issues relating to information security incidents; □ any remedies that can apply if certain information security incidents occur.	Incident Response Framework	The organization maintains a framework that defines how to organize a response to security & privacy incidents.	Integrity, Availability, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 16.1.1-P Responsibilities and procedures	27017 - Provider Implementation Guidance: As a part of the service specifications, the cloud service provider should define the allocation of information security incident management responsibilities and procedures between the cloud service customer and the cloud service provider. The cloud service provider should provide the cloud service customer with documentation covering: □ the scope of information security incidents that the cloud service provider will report to the cloud service customer; □ the level of disclosure of the detection of information security incidents and the associated responses; □ the target timeframe in which notifications of informationsecurity incidents will occur; □ the procedure for the notification of information security incidents; □ contact information for the handling of issues relating to information security incidents; □ any remedies that can apply if certain information security incidents occur.	Incident Response Policy - Management's Responsibility	The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 16.1.2-P Reporting information security events	27017 - Provider Implementation Guidance: The cloud service provider should provide mechanisms for: □ the cloud service customer to report an information security event to the cloud service provider; □ the cloud service provider to report an information security event to a cloud service customer; □ the cloud service customer to track the status of a reported information security event.	Incident Response Policy - Management's Responsibility	The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 16.1.2-P Reporting information security events	27017 - Provider Implementation Guidance: The cloud service provider should provide mechanisms for: □ the cloud service customer to report an information security event to the cloud service provider; □ the cloud service provider to report an information security event to a cloud service customer; □ the cloud service customer to track the status of a reported information security event.	Incident Reporting External	The organization provides external users with mechanisms to report security issues, incidents and concerns.	Availability, Confidentiality, Integrity	Risk, Contractual, Regulatory, Culture

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27017:2015	[ISO 27017] 16.1.2-P Reporting information security events	27017 - Provider Implementation Guidance: The cloud service provider should provide mechanisms for: □ the cloud service customer to report an information security event to the cloud service provider; □ the cloud service provider to report an information security event to a cloud service customer; □ the cloud service customer to track the status of a reported information security event.	Security Team Engagement	The organization has established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.	Security	Risk, Contractual, Regulatory, Culture
ISO/IEC 27017:2015	[ISO 27017] 16.1.7-P Collection of evidence	27017 - Provider Implementation Guidance: The cloud service customer and the cloud service provider should agree upon the procedures to respond to requests for potential digital evidence or other information from within the cloud computing environment.	Incident Response Policy - Management's Responsibility	The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 18.1.1-P Identification of applicable legislation and contractual requirements	27017 - Provider Implementation Guidance: The cloud service provider should inform the cloud service customer of the legal jurisdictions governing the cloud service. The cloud service provider should identify its own relevant legal requirements (e.g., regarding encryption to protect personally identifiable information (PII)) This information should also be provided to the cloud service customer when requested. The cloud service provider should provide the cloud service customer with evidence of its current compliance with applicable legislation and contractual requirements.	Identification of applicable legislation and contractual requirements	The approach to meeting relevant statutory, regulatory, and contractual requirements is defined, documented, and kept up to date for each system and organization through review by appropriate Product Counsels.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 18.1.2-P Intellectual property rights	27017 - Provider Implementation Guidance: The cloud service provider should establish a process for responding to intellectual property rights complaints.	Intellectual property rights	The organization has policies and guidelines in place which govern the use of intellectual property and third-party software. The organization utilizes software management systems to install software and track usage.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 18.1.3-P Protection of records	27017 - Provider Implementation Guidance: The cloud service provider should provide information to the cloud service customer about the protection of records that are gathered and stored by the cloud service provider relating to the use of cloud services by the cloud service customer.	Protection of records	The organization has information security and data access policies and controls in place to prevent unauthorized access, alteration, disclosure, or destruction of important records.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 18.1.5-P Regulation of cryptographic controls	27017 - Provider Implementation Guidance: The cloud service provider should provide descriptions of the cryptographic controls implemented by the cloud service provider to the cloud service customer for reviewing compliance with applicable agreements, legislation and regulations.	Regulation of cryptographic controls	The organization ensures that cryptographic controls are used in compliance with relevant agreements, laws, and regulations.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] 18.2.1-P Independent review of information security	27017 - Provider Implementation Guidance: The cloud service provider should provide documented evidence to the cloud service customer to substantiate its claim of implementing information security controls. Where individual cloud service customer audits are impractical or can increase risks to information security, the cloud service provider should provide independent evidence that information security is implemented and operated in accordance with the cloud service provider's policies and procedures. This should be made available to prospective cloud service customers prior to entering a contract. A relevant independent audit as selected by the cloud service provider should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the cloud service provider's operations, provided sufficient transparency is provided. When the independent audit is impractical, the cloud service provider should conduct a self-assessment, and disclose its process and results to the cloud service customer.	Independent review of information security	The organization has an internal audit function and regularly engages independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27017:2015	[ISO 27017] A.6.3.1-P Shared roles and responsibilities within a cloud computing environment	27017 - Provider Implementation Guidance: The cloud service provider should document and communicate its information security capabilities, roles, and responsibilities for the use of its cloud service, along with the information security roles and responsibilities for which the cloud service customer would need to implement and manage as part of its use of the cloud service.	Shared responsibility within a cloud computing environment	The organization provides information pertaining to the shared responsibilities of both itself and the cloud service customer.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] A.8.1.5-P Removal of cloud service customer assets	27017 - Provider Implementation Guidance: The cloud service provider should provide information about the arrangements for the return and removal of any cloud service customer's assets upon termination of the agreement for the use of a cloud service. The asset return and removal arrangements should be documented in the agreement and should be performed in a timely manner. The arrangements should specify the assets to be returned and removed.	Removal of cloud service customer assets	The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Confidentiality, Privacy	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] A.9.5.1-P Segregation in virtual computing environments	27017 - Provider Implementation Guidance: The cloud service provider should enforce appropriate logical segregation of cloud service customer data, virtualized applications, operating systems, storage, and network for: □ the separation of resources used by cloud service customers in multi-tenant environments; □ the separation of the cloud service provider's internal administration from resources used by cloud service customers. Where the cloud service involves multi-tenancy, the cloud service provider should implement information security controls to ensure appropriate isolation of resources used by different tenants. The cloud service provider should consider the risks associated with running cloud service customer-supplied software within the cloud services offered by the cloud service provider.	Segregation in virtual computing environments	The organization has implemented mechanisms to protect a customer's environment from other customers and unauthorized persons.	Confidentiality	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] A.9.5.2-P Virtual machine hardening	27017 - Provider Implementation Guidance: When configuring virtual machines, cloud service customers and cloud service providers should ensure that appropriate aspects are hardened (e. g., only those ports, protocols and services that are needed), and that the appropriate technical measures are in place (e.g., anti-malware, logging) for each virtual machine used.	Virtual Machine Hardening	The organization hardens virtual environments where it has a responsibility as outlined in the shared responsibilities.	Availability, Confidentiality, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] A.12.1.5-P Administrator's operational security	27017 - Provider Implementation Guidance: The cloud service provider should provide documentation about the critical operations and procedures to cloud service customers who require it.	Administrator’s operational security	Procedures for administrative operations of the organization's cloud computing environment are documented and provided to customers.	Confidentiality, Privacy, Availability, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] A.12.4.5-P Monitoring of Cloud Services	27017 - Provider Implementation Guidance: The cloud service provider should provide capabilities that enable the cloud service customer to monitor specified aspects, relevant to the cloud service customer, of the operation of the cloud services. For example, to monitor and detect if the cloud service is being used as a platform to attack others, or if sensitive data is being leaked from the cloud service. Appropriate access controls should secure the use of the monitoring capabilities. The capabilities should provide access only to information about the cloud service customer's own cloud service instances. The cloud service provider should provide documentation of the service monitoring capabilities to the cloud service customer. Monitoring should provide data consistent with the event logs described in clause 12.4.1 and assist with SLA terms.	Monitoring of Cloud Services	The organization provides monitoring capabilities for customers of cloud services.	Availability, Confidentiality	Regulatory, Contractual, Risk

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27017:2015	[ISO 27017] A.13.1.4-P Alignment of security management for virtual and physical networks	27017 - Provider Implementation Guidance: The cloud service provider should define and document an information security policy for the configuration of the virtual network consistent with the information security policy for the physical network. The cloud service provider should ensure that the virtual network configuration matches the information security policy regardless of the means used to create the configuration.	Security policy for physical and virtual networks	The organization's network security policies and guidelines apply to both physical and virtual networks.	Confidentiality	Regulatory, Contractual, Risk
ISO/IEC 27017:2015	[ISO 27017] 9.4.1-P Information Access Restriction	27017 - Provider Implementation Guidance: The cloud service provider should provide access controls that allow the cloud service customer to restrict access to its cloud services, its cloud service functions and the cloud service customer data maintained in the service.	Access with least privilege	The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory