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 27001:2022	[ISO 27001] A.5.1 Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	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 27001:2022	[ISO 27001] A.5.1 Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Review of the policies for information security	Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.2 Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	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 27001:2022	[ISO 27001] A.5.3 Segregation of duties	Conflicting duties and areas of responsibility should be segregated.	Segregation of duties	The organization separates duties of individuals by granting users access based on job responsibilities and least privilege, and limiting access to only authorized users.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.4 Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Data Center Security review	Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.4 Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Code of Conduct acknowledgement	Personnel of the organization are required to acknowledge the code of conduct.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.5 Contact with authorities	The organization should establish and maintain contact with relevant authorities.	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 27001:2022	[ISO 27001] A.5.6 Contact with special interest groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Contact with special interest groups	The organization is an active participant in the security industry and maintains appropriate contacts with special interest groups, security forums, and professional associations.	Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.7 Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	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 27001:2022	[ISO 27001] A.5.7 Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	Threat intelligence and prevention	A dedicated function is in place to produce insights (intelligence), and implement protections to reduce the risk that threat actors pose to the organization.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.8 Information security in project management	Information security should be integrated into project management.	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 27001:2022	[ISO 27001] A.5.8 Information security in project management	Information security should be integrated into project management.	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 27001:2022	[ISO 27001] A.5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Information Stewardship	The primary information assets within the ISMS are owned by the organization's customer and users. The organization serves as a steward of that information in compliance with the published Terms of Service.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Ownership of assets	The Technical Infrastructure Product Area ultimately owns assets used for information processing (i.e. production machines). Assets are allocated to individual teams upon request.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Inventory of corporate endpoint assets	The organization maintains an up-to-date, accurate client device inventory	Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.10 Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Acceptable use of assets	The organization has policies and guidelines that govern the acceptable use of information assets.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.10 Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Data Classification	The organization has established policies and guidelines to govern data classification, labeling and security.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.11 Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Monitoring for security threats	The organization monitors its networks and systems for threats to information security.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.11 Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Offboarding procedures	The organization has established an offboarding procedure for personnel, which governs the removal of access and return of assets.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.11 Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	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 27001:2022	[ISO 27001] A.5.11 Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Access revoked on Exit	Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis upon submission of a termination request by Human Resources or a manager.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.12 Classification of information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Data Classification	The organization has established policies and guidelines to govern data classification, labeling and security.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.13 Labelling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Data Classification	The organization has established policies and guidelines to govern data classification, labeling and security.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.14 Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Electronic messaging	The organization's internal email systems are protected by anti-spam, anti-phishing & anti-malware mechanisms.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.14 Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Information transfer policies and procedures	The organization has policies and guidelines in place for the exchange of information.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.14 Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	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 27001:2022	[ISO 27001] A.5.14 Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	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 27001:2022	[ISO 27001] A.5.14 Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Securing hard copy material	The organization has security policies and guidelines around office security practices, including securing any hard copy (printed) documents and removable media.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001:2022	[ISO 27001] A.5.14 Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	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 27001:2022	[ISO 27001] A.5.14 Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Vendor Security Assessment	The Privacy, Safety Security Org (PSS) takes a risk based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	Security Integrity Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.15 Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Access control policy	The organization has policies and guidelines that govern access to information systems.	Availability, Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.15 Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Access to networks and network services	The organization has a policy to reduce the risk of compromise to its data and infrastructure from devices connected to internal networks.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.16 Identity management	The full life cycle of identities should be managed.	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 27001:2022	[ISO 27001] A.5.16 Identity management	The full life cycle of identities should be managed.	Access control policy	The organization has policies and guidelines that govern access to information systems.	Availability, Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.17 Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel of appropriate handling of authentication information.	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
ISO/IEC 27001:2022	[ISO 27001] A.5.17 Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel of appropriate handling of authentication information.	Password management system	The organization has a password change system that enforces its password guidelines.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.18 Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	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 27001:2022	[ISO 27001] A.5.18 Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	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 27001:2022	[ISO 27001] A.5.18 Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Periodic Access Review	Critical access groups are reviewed on a periodic basis and inappropriate access is removed.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.18 Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	User Access on Demand	Where "on demand request" mechanisms are implemented to restrict human access to production resources, access requests are reviewed and approved by a second individual prior to being granted and the event is logged.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.19 Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	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 27001:2022	[ISO 27001] A.5.19 Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	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 27001:2022	[ISO 27001] A.5.19 Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	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 27001:2022	[ISO 27001] A.5.19 Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Supplier offboarding	The organization has procedures in place to ensure the secure termination of suppliers.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.19 Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Vendor Security Assessment	The Privacy, Safety Security Org (PSS) takes a risk based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	Security Integrity Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.19 Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Security Assessment of Vendor Facilities	Vendor facilities are assessed for security.	Confidentiality, Security	Risk, Culture, Contractual
ISO/IEC 27001:2022	[ISO 27001] A.5.20 Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	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 27001:2022	[ISO 27001] A.5.20 Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	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 27001:2022	[ISO 27001] A.5.20 Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	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 27001:2022	[ISO 27001] A.5.20 Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Vendor Security Assessment	The Privacy, Safety Security Org (PSS) takes a risk based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	Security Integrity Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.21 Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage information security risks associated with the ICT products and services supply chain.	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 27001:2022	[ISO 27001] A.5.21 Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage information security risks associated with the ICT products and services supply chain.	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 27001:2022	[ISO 27001] A.5.21 Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage information security risks associated with the ICT products and services supply chain.	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 27001:2022	[ISO 27001] A.5.21 Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage information security risks associated with the ICT products and services supply chain.	Vendor Security Assessment	The Privacy, Safety Security Org (PSS) takes a risk based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessment as determined by the sensitivity of data being processed or access being granted.	Security Integrity Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.22 Monitoring, review and change management of supplier services	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Policies & procedures for third parties	The organization has policies and guidelines that govern third-party relationships.	Availability, Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.23 Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with organization's information security requirements.	Policies for use of cloud services	The organization has established policies and procedures that govern the acquisition, use, management and exit from cloud services.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001:2022	[ISO 27001] A.5.23 Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with organization's information security requirements.	Policies & procedures for third parties	The organization has policies and guidelines that govern third-party relationships.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.24 Information security incident management planning and preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	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 27001:2022	[ISO 27001] A.5.25 Assessment and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents.	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 27001:2022	[ISO 27001] A.5.26 Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	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 27001:2022	[ISO 27001] A.5.27 Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Learning from information security incidents	Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen & improve security controls, prevent future incidents, and can be used as examples for information security training.	Integrity, Availability, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.28 Collection of evidence	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	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 27001:2022	[ISO 27001] A.5.29 Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Continuity of security operations	The organization has implemented a "follow the sun" model for its Security & Privacy Incident Response teams to ensure 24x7 coverage & continuity of operations.	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.29 Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Information security continuity	The organization has geographically dispersed personnel responsible for managing security incidents.	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.29 Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	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 27001:2022	[ISO 27001] A.5.29 Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Disaster recovery testing	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.29 Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Data restore tests	Restore tests are periodically performed to confirm the ability to recover user data.	Availability, Integrity, Privacy	Risk, Regulatory, Contractual
ISO/IEC 27001:2022	[ISO 27001] A.5.30 ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Disaster recovery testing	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.30 ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	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 27001:2022	[ISO 27001] A.5.30 ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Data restore tests	Restore tests are periodically performed to confirm the ability to recover user data.	Availability, Integrity, Privacy	Risk, Regulatory, Contractual
ISO/IEC 27001:2022	[ISO 27001] A.5.31 Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	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 27001:2022	[ISO 27001] A.5.31 Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	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 27001:2022	[ISO 27001] A.5.32 Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	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 27001:2022	[ISO 27001] A.5.33 Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	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 27001:2022	[ISO 27001] A.5.34 Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Privacy and protection of identifiable data	The organization has policies and guidelines in place which govern the use and protection of identifiable data.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.35 Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	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 27001:2022	[ISO 27001] A.5.36 Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	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 27001:2022	[ISO 27001] A.5.36 Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	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 27001:2022	[ISO 27001] A.5.36 Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	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 27001:2022	[ISO 27001] A.5.36 Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	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 27001:2022	[ISO 27001] A.5.36 Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Product launch process	Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.5.37 Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Documented operating procedures	Teams within the organization document standard operating procedures and make them available to authorized personnel	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.1 Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Background Checks	Background checks are performed on new hires as permitted by local laws.	Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.2 Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	Code of Conduct acknowledgement	Personnel of the organization are required to acknowledge the code of conduct.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.3 Information security awareness, education and training	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic specific policies and procedures, as relevant for their job function.	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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001:2022	[ISO 27001] A.6.4 Disciplinary process	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	Disciplinary process	The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.4 Disciplinary process	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	Confidentiality agreements with employees	The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.5 Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the all personnel and enforced.	Code of Conduct acknowledgement	Personnel of the organization are required to acknowledge the code of conduct.	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.5 Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the all personnel and enforced.	Offboarding procedures	The organization has established an offboarding procedure for personnel, which governs the removal of access and return of assets.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.6 Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Confidentiality agreements with extended workforce	The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.6 Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Confidentiality agreements with employees	The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.7 Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Teleworking	The organization has established guidelines for protecting against the risks of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.7 Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Remote Access	Remote access to corporate machines requires a digital certificate issued by the organization installed on the connecting device, and two-factor authentication in the form of user ID, password, security key, and/or certificate.	Security	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.6.8 Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	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 27001:2022	[ISO 27001] A.6.8 Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Incident Response Framework	The organization maintains a framework that defines how to organize a response to security & privacy incidents.	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.1 Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Monitoring physical key usage	Use of physical keys to access high security areas in data centers result in alerts to security personnel.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.1 Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	DC physical security	Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.1 Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Security perimeter	Data center perimeters are defined and secured via physical barriers.	Confidentiality, Availability, Integrity	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.1 Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Physical security perimeter	Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.	Availability, Confidentiality, Integrity	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.2 Physical entry	Secure areas should be protected by appropriate entry controls and access points.	DC Visitor escort	Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.2 Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Delivery and loading areas	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.	Availability, Integrity, Confidentiality	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.2 Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Office physical entry controls	Visitors to corporate offices must be authenticated upon arrival and remain with an escort for the duration of their visit.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.2 Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Data center ACL review	Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.2 Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Physical access logs are recorded	Data center physical access logs are recorded and retained in accordance with organizational or regulatory requirements.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.2 Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Monitoring physical key usage	Use of physical keys to access high security areas in data centers result in alerts to security personnel.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	Monitoring physical key usage	Use of physical keys to access high security areas in data centers result in alerts to security personnel.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	Securing offices, rooms and facilities	Physical access to the Corporate Offices is secured via security personnel, badge readers, security credentials (badges) and/or video cameras.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.4 Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	DC physical security	Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.5 Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	External & environmental threats	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.5 Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	Office fire detection & protection	Corporate offices are equipped with fire detection alarms and protection equipment.	Availability	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.5 Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	Fire detection & protection	Data centers are equipped with fire detection alarms and protection equipment.	Availability	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.6 Working in secure areas	Security measures for working in secure areas should be designed and implemented.	Working in secure areas	The organization has policies and guidelines for working in secure areas.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.7 Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Securing hard copy material	The organization has security policies and guidelines around office security practices, including securing any hard copy (printed) documents and removable media.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.7 Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Securing unattended workstations	The organization has security policies that require users to lock their workstations and mobile devices when unattended.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.8 Equipment siting and protection	Equipment should be sited securely and protected.	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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001:2022	[ISO 27001] A.7.9 Security of assets off-premises	Off-site assets should be protected.	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 27001:2022	[ISO 27001] A.7.9 Security of assets off-premises	Off-site assets should be protected.	Control of Asset Deliveries	The organization authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items. * Deliveries of Assets GPN's IN and Out of DC's	Confidentiality, Integrity, Availability	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.9 Security of assets off-premises	Off-site assets should be protected.	Mobile device policy	The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.10 Storage media	Storage media should be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Automated asset & inventory tracking	Automated mechanisms are utilized to track inventory of all production machines and inventory of all serialized server components.	Availability, Integrity, Confidentiality	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.10 Storage media	Storage media should be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Control of Asset Deliveries	The organization authorizes, monitors, and controls all information systems and data center equipment entering and exiting data centers and maintains records of those items. * Deliveries of Assets GPN's IN and Out of DC's	Confidentiality, Integrity, Availability	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.10 Storage media	Storage media should be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Management of removable media	The organization has guidelines in place for the management and use of removable media.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.10 Storage media	Storage media should be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	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 27001:2022	[ISO 27001] A.7.11 Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Supporting utilities	Power management and distribution systems are utilized to protect critical data center equipment from disruption or damage.	Availability	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.12 Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Office cabling security	Critical power and telecommunications equipment in corporate offices is physically protected from disruption and damage.	Availability	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.12 Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Cabling security	Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.	Integrity, Availability, Confidentiality	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.13 Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Equipment maintenance	Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.	Integrity, Availability	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.7.14 Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	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 27001:2022	[ISO 27001] A.8.1 User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Unattended user equipment	The organization has a security guideline that requires users to lock their workstations and mobile devices when unattended. Access to unattended workstations is prevented by a password protected screen-saver after 15 minutes of inactivity.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.1 User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Securing unattended workstations	The organization has security policies that require users to lock their workstations and mobile devices when unattended.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.1 User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Mobile device policy	The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.2 Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	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 27001:2022	[ISO 27001] A.8.3 Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	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
ISO/IEC 27001:2022	[ISO 27001] A.8.4 Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.	Source code change management tools	The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.5 Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Secure log-on procedures	Personnel access to sensitive internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.6 Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	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 27001:2022	[ISO 27001] A.8.6 Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Monitoring for Operational Issues	The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Security	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.6 Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Operations monitoring tool alerts	Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Security	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.7 Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	Protections against malicious activity	The organization has implemented mechanisms to protect its information assets against malicious activity (e.g. malware, spam, phishing).	Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.8 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	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 27001:2022	[ISO 27001] A.8.9 Configuration management	Configuration, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Network change review	Changes to network configurations are reviewed and approved prior to deployment.	Availability, Confidentiality, Integrity	Risk, Contractual, Culture, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.9 Configuration management	Configuration, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	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 27001:2022	[ISO 27001] A.8.9 Configuration management	Configuration, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	OS deviation	Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.	Integrity	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.9 Configuration management	Configuration, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Encryption of Corporate Managed Endpoints	The organization encrypts corporate managed endpoints during the initial device setup process and ensures the device remains encrypted throughout its lifecycle.	Confidentiality, Integrity	Regulatory, Contractual, Risk
ISO/IEC 27001:2022	[ISO 27001] A.8.9 Configuration management	Configuration, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Standard Image on Prod	A standard image is utilized for the installation and maintenance of each production server.	Security	Regulatory, Contractual, Risk
ISO/IEC 27001:2022	[ISO 27001] A.8.10 Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Data retention and deletion policy	The organization has procedures in place to dispose of confidential and need to know (ntk) information according to the data retention and deletion policy.	Confidentiality, Privacy	Risk, Culture, Contractual

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001:2022	[ISO 27001] A.8.10 Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	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 27001:2022	[ISO 27001] A.8.10 Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Mobile device policy	The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.10 Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Encryption of Corporate Managed Endpoints	The organization encrypts corporate managed endpoints during the initial device setup process and ensures the device remains encrypted throughout its lifecycle.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.11 Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related ones, and business requirements, taking legal requirements into consideration.	Data anonymization guidelines	The organization maintains policies that define the requirements for the use of data anonymization.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.11 Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related ones, and business requirements, taking legal requirements into consideration.	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 27001:2022	[ISO 27001] A.8.11 Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related ones, and business requirements, taking legal requirements into consideration.	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
ISO/IEC 27001:2022	[ISO 27001] A.8.12 Data leakage prevention	These measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	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, Contractual, Culture
ISO/IEC 27001:2022	[ISO 27001] A.8.12 Data leakage prevention	These measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Monitoring for security threats	The organization monitors its networks and systems for threats to information security.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.13 Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	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 27001:2022	[ISO 27001] A.8.13 Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Data restore tests	Restore tests are periodically performed to confirm the ability to recover user data.	Availability, Integrity, Privacy	Risk, Regulatory, Contractual
ISO/IEC 27001:2022	[ISO 27001] A.8.13 Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Disaster recovery testing	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.14 Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	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 27001:2022	[ISO 27001] A.8.15 Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Security logs are protected and access restricted	Security event logs are protected and access is restricted to authorized personnel.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.15 Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	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 27001:2022	[ISO 27001] A.8.15 Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Administrator and operator logs	Audit logs are retained for the following auditable events: privileged user access activities, authorized access attempts, and unauthorized access attempts.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.16 Monitoring activities	Networks, systems and applications should be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	Monitoring for security threats	The organization monitors its networks and systems for threats to information security.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.16 Monitoring activities	Networks, systems and applications should be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	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 27001:2022	[ISO 27001] A.8.17 Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Clock synchronisation	Internal system clocks are synchronized to atomic clocks and GPS.	Integrity	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.18 Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	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 27001:2022	[ISO 27001] A.8.19 Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	OS deviation	Deviations from pre-defined operating system (OS) configurations running on production machines are detected and corrected.	Integrity	Risk, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.19 Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Installation of software on operational systems	The organization has established guidelines for governing the installation of software on organization-owned assets.	Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.19 Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	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 27001:2022	[ISO 27001] A.8.19 Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Standard Image on Prod	A standard image is utilized for the installation and maintenance of each production server.	Security	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.20 Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Encryption of data-in-transit between the organization's production facilities	The organization uses encryption to secure user data in transit between the organization's production facilities.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.20 Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Perimeter devices	The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.21 Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Security of network services	The organization has dedicated teams who are responsible for monitoring, maintaining, managing and securing the network.	Integrity, Availability, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.21 Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Monitoring for Operational Issues	The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Security	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.21 Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Operations monitoring tool alerts	Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Security	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.22 Segregation of networks	Groups of information services, users and information systems should be segregated in the organization's networks.	Security of Wireless Networks	Wireless connections to Corp resources at organization's facilities are encrypted	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.22 Segregation of networks	Groups of information services, users and information systems should be segregated in the organization's networks.	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 27001:2022	[ISO 27001] A.8.23 Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Electronic messaging	The organization's internal email systems are protected by anti-spam, anti-phishing & anti-malware mechanisms.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001:2022	[ISO 27001] A.8.23 Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Protections against malicious activity	The organization has implemented mechanisms to protect its information assets against malicious activity (e.g. malware, spam, phishing).	Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.23 Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Protections against malicious external web content	The organization has a counter abuse function that is responsible for implementing policies and technologies related to protecting against malicious web content.	Confidentiality, Availability, Integrity	Risk, Contractural, Culture
ISO/IEC 27001:2022	[ISO 27001] A.8.24 Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Policy on the use of cryptographic controls	The organization maintains policies that define the requirements for the use of cryptography.	Confidentiality, Privacy, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.24 Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Key management	The organization has an established key management process in place to support the organization's use of cryptographic techniques.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.25 Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	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 27001:2022	[ISO 27001] A.8.26 Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Key management	The organization has an established key management process in place to support the organization's use of cryptographic techniques.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.26 Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Encryption of data-in-transit between users and the organization's production facilities	The organization uses encryption protocols to secure user data in transit between users and the organization's production facilities	Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.26 Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	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 27001:2022	[ISO 27001] A.8.26 Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Encryption at rest	Customer data that is uploaded or created is encrypted at rest.	Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.27 Secure system architecture and engineering principles	Principles for engineering secure systems x be established, documented, maintained and applied to any information system development activities.	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 27001:2022	[ISO 27001] A.8.28 Secure coding	Secure coding principles should be applied to software development.	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 27001:2022	[ISO 27001] A.8.29 Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	System security testing	The organization tests, validates, and documents changes to its services prior to deployment to production.	Availability, Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.29 Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	Changes are tested	Changes to the organization's systems are tested before being deployed.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.30 Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	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 27001:2022	[ISO 27001] A.8.30 Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	Disciplinary process	The organization has established a disciplinary process to address non-compliance with company policies, the code of conduct, or other personnel requirements.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.30 Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	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 27001:2022	[ISO 27001] A.8.30 Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	Product launch process	Design documentation is required to be completed and be reviewed before a feature launch which introduces new collection, processing, or sharing of user data.	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.31 Separation of development, test and production environments	Development, testing and production environments should be separated and secured.	Source code change management tools	The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.31 Separation of development, test and production environments	Development, testing and production environments should be separated and secured.	Separation of development, testing and operational environments	Development, testing and build environments are separated from the production environment through the use of logical security controls.	Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.32 Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Changes are tested	Changes to the organization's systems are tested before being deployed.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.32 Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Review System Changes	System changes are reviewed and approved by a separate technical resource before moving into production.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.32 Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	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 27001:2022	[ISO 27001] A.8.33 Test information	Test information should be appropriately selected, protected and managed.	Separation of development, testing and operational environments	Development, testing and build environments are separated from the production environment through the use of logical security controls.	Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001:2022	[ISO 27001] A.8.34 Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Information systems audit controls	The organization plans and coordinates system security-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users.	Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory