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: 2013	[ISO 27001] A.5.1.1 Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	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: 2013	[ISO 27001] A.5.1.2 Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	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: 2013	[ISO 27001] A.6.1.1 Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	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	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.6.1.2 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	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: 2013	[ISO 27001] A.6.1.3 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	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: 2013	[ISO 27001] A.6.1.4 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	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	Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.6.1.5 Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	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: 2013	[ISO 27001] A.6.2.1 Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	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: 2013	[ISO 27001] A.6.2.2 Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	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	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.7.1.1 Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements,	Background Checks	Background checks are performed on new hires as permitted by local laws.	Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.7.1.2 Terms and conditions of employment	The contractual agreements with employees and contractors shall state their 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: 2013	[ISO 27001] A.7.2.1 Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established 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: 2013	[ISO 27001] A.7.2.1 Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established 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: 2013	[ISO 27001] A.7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as	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: 2013	[ISO 27001] A.7.2.3 Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	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: 2013	[ISO 27001] A.7.3.1 Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor 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: 2013	[ISO 27001] A.7.3.1 Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor 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: 2013	[ISO 27001] A.8.1.1 Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up 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: 2013	[ISO 27001] A.8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.	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	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.	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	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.8.1.3 Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall 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: 2013	[ISO 27001] A.8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon 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: 2013	[ISO 27001] A.8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon 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: 2013	[ISO 27001] A.8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon 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	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001: 2013	[ISO 27001] A.8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon 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: 2013	[ISO 27001] A.8.2.1 Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	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: 2013	[ISO 27001] A.8.2.2 Labelling of information	An appropriate set of procedures for information labeling shall 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: 2013	[ISO 27001] A.8.2.3 Handling of assets	Procedures for handling assets shall 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: 2013	[ISO 27001] A.8.3.1 Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	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: 2013	[ISO 27001] A.8.3.2 Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	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: 2013	[ISO 27001] A.8.3.3 Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Storage media transfer	Storage media used for off-site redundancy are protected and controlled during transport outside of controlled areas using secure storage containers.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.9.1.1 Access control policy	An access control policy shall be established, documented and reviewed 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: 2013	[ISO 27001] A.9.1.2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	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: 2013	[ISO 27001] A.9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	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: 2013	[ISO 27001] A.9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	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	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and 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	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.9.2.4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	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: 2013	[ISO 27001] A.9.2.4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Password management system	The organization has a password change system that enforces its password guidelines.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.	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: 2013	[ISO 27001] A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.	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	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or	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: 2013	[ISO 27001] A.9.3.1 Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret 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: 2013	[ISO 27001] A.9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	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	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	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: 2013	[ISO 27001] A.9.4.3 Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Password management system	The organization has a password change system that enforces its password guidelines.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall 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	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.9.4.5 Access control to program source code	Access to program source code shall be restricted.	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: 2013	[ISO 27001] A.10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed 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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001: 2013	[ISO 27001] A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	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: 2013	[ISO 27001] A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	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: 2013	[ISO 27001] A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Security perimeter	Data center perimeters are defined and secured via physical barriers.	Confidentiality, Availability, Integrity	Risk, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	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: 2013	[ISO 27001] A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	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: 2013	[ISO 27001] A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	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: 2013	[ISO 27001] A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	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	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	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: 2013	[ISO 27001] A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	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: 2013	[ISO 27001] A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	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: 2013	[ISO 27001] A.11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	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: 2013	[ISO 27001] A.11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	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: 2013	[ISO 27001] A.11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	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: 2013	[ISO 27001] A.11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Office fire detection & protection	Corporate offices are equipped with fire detection alarms and protection equipment.	Availability	Risk, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Fire detection & protection	Data centers are equipped with fire detection alarms and protection equipment.	Availability	Risk, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Working in secure areas	The organization has policies and guidelines for working in secure areas.	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing	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: 2013	[ISO 27001] A.11.2.1 Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Equipment siting and protection	The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.2.2 Supporting utilities	Equipment shall 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: 2013	[ISO 27001] A.11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall 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: 2013	[ISO 27001] A.11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall 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: 2013	[ISO 27001] A.11.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Equipment maintenance	Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including	Integrity, Availability	Risk, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Automated inventory tracking	Automated mechanisms are utilized to track inventory of production machines and inventory of all serialized server components.	Availability, Integrity, Confidentiality	Risk, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	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.	Confidentiality, Integrity, Availability	Risk, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001: 2013	[ISO 27001] A.11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	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.	Confidentiality, Integrity, Availability	Risk, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	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: 2013	[ISO 27001] A.11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Storage media transfer	Storage media used for off-site redundancy are protected and controlled during transport outside of controlled areas using secure storage containers.	Confidentiality, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.2.7 Secure disposal or re-use of equipment	All items of equipment containing storage media shall 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: 2013	[ISO 27001] A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	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	Confidentiality, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	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: 2013	[ISO 27001] A.11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	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: 2013	[ISO 27001] A.11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	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: 2013	[ISO 27001] A.12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users 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: 2013	[ISO 27001] A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	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: 2013	[ISO 27001] A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Change management policies	The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Changes are tested	Changes to the organization's systems are tested before being deployed.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Monitoring Git-on-Borg changes for approvals	Git-on-Borg code changes are monitored for approvals on a periodic basis.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.12.1.3 Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	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	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	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: 2013	[ISO 27001] A.12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	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: 2013	[ISO 27001] A.12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with 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: 2013	[ISO 27001] A.12.3.1 Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup pol	Service Redundancy	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and	Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	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: 2013	[ISO 27001] A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	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: 2013	[ISO 27001] A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	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: 2013	[ISO 27001] A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	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: 2013	[ISO 27001] A.12.4.4 Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Clock synchronisation	Internal system clocks are synchronized to atomic clocks and GPS.	Integrity	Risk, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software 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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001: 2013	[ISO 27001] A.12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software 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: 2013	[ISO 27001] A.12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate	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: 2013	[ISO 27001] A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	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	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	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: 2013	[ISO 27001] A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	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: 2013	[ISO 27001] A.12.7.1 Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	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	Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.13.1.1 Network controls	Networks shall be 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: 2013	[ISO 27001] A.13.1.1 Network controls	Networks shall be 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: 2013	[ISO 27001] A.13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are	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: 2013	[ISO 27001] A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on 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	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on 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: 2013	[ISO 27001] A.13.2.1 Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	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: 2013	[ISO 27001] A.13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Subprocessor obligations to safeguard customer data and service data where Google is a processor	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: 2013	[ISO 27001] A.13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external 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: 2013	[ISO 27001] A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	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: 2013	[ISO 27001] A.13.2.4 Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	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: 2013	[ISO 27001] A.13.2.4 Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	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	Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.14.1.1 Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	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: 2013	[ISO 27001] A.14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	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: 2013	[ISO 27001] A.14.1.3 Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure,	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: 2013	[ISO 27001] A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	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: 2013	[ISO 27001] A.14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Monitoring Git-on-Borg changes for approvals	Git-on-Borg code changes are monitored for approvals on a periodic basis.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001: 2013	[ISO 27001] A.14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control 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.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Change management policies	The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Changes are tested	Changes to the organization's systems are tested before being deployed.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	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: 2013	[ISO 27001] A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Monitoring Git-on-Borg changes for approvals	Git-on-Borg code changes are monitored for approvals on a periodic basis.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Monitoring Git-on-Borg changes for approvals	Git-on-Borg code changes are monitored for approvals on a periodic basis.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Change management policies	The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.14.2.5 Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	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: 2013	[ISO 27001] A.14.2.6 Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	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: 2013	[ISO 27001] A.14.2.6 Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	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: 2013	[ISO 27001] A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of 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: 2013	[ISO 27001] A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of 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: 2013	[ISO 27001] A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of 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: 2013	[ISO 27001] A.14.2.8 System security testing	Testing of security functionality shall be carried out during development.	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: 2013	[ISO 27001] A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Changes are tested	Changes to the organization's systems are tested before being deployed.	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	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: 2013	[ISO 27001] A.14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled.	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: 2013	[ISO 27001] A.15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	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: 2013	[ISO 27001] A.15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	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: 2013	[ISO 27001] A.15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Subprocessor obligations to safeguard customer data and service data where Google is a processor	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: 2013	[ISO 27001] A.15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the	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

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001: 2013	[ISO 27001] A.15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the	Subprocessor obligations to safeguard customer data and service data where Google is a processor	The organization requires subprocessors to meet security & privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are	Availability, Confidentiality, Integrity, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the	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	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.15.1.3 Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Subprocessor obligations to safeguard customer data and service data where Google is a processor	The organization requires subprocessors to meet security & privacy requirements for safeguarding customer data and service data where Google is a processor. Requirements are	Availability, Confidentiality, Integrity, Privacy	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.15.1.3 Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product 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: 2013	[ISO 27001] A.15.1.3 Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product 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	Privacy, Integrity, Confidentiality, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.15.2.1 Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier 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: 2013	[ISO 27001] A.15.2.2 Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the	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: 2013	[ISO 27001] A.16.1.1 Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	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,	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	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,	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.16.1.3 Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems	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,	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.16.1.4 Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified 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: 2013	[ISO 27001] A.16.1.5 Response to information security incidents	Information security incidents shall 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,	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.16.1.6 Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Learning from information security incidents	Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to prevent future incidents and can be	Integrity, Availability, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	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,	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	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,	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Information security continuity	The organization has geographically dispersed personnel responsible for managing security incidents.	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	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,	Confidentiality, Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Information security continuity	The organization has geographically dispersed personnel responsible for managing security incidents.	Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	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: 2013	[ISO 27001] A.17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	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: 2013	[ISO 27001] A.17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	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: 2013	[ISO 27001] A.17.2.1 Availability of information processing facilities	Information processing facilities shall 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	Integrity, Availability	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.18.1.1 Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up	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	Confidentiality, Availability, Integrity	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.18.1.2 Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	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	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory

Standard Title	Requirement Title	Requirement Description	Control Title	Control Description	Control Assertions	Rationale for Inclusion
ISO/IEC 27001: 2013	[ISO 27001] A.18.1.3 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	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: 2013	[ISO 27001] A.18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	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: 2013	[ISO 27001] A.18.1.5 Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Regulation of cryptographic controls	The organization ensures that cryptographic controls are used in compliance with relevant agreements, laws, and regulations.	Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.18.2.1 Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be	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	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory
ISO/IEC 27001: 2013	[ISO 27001] A.18.2.2 Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security	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: 2013	[ISO 27001] A.18.2.2 Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security	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: 2013	[ISO 27001] A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	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	Availability, Integrity, Confidentiality	Risk, Culture, Contractual, Regulatory