INSTRUCTURE

Statement Of Applicability
(ISO 27001:2013)

ISO 27001 Clause #	Title	Control	Applicability [Y/N]	Controlled by 3rd Party	3rd Party Name	Selection Justification/Exclusion - Explanation	Remarks
A.5	**Information Security Policy**						
A.5.1	*Management Directions for Information Security*	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.					
A.5.1.1	Policies for information security	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	Y			Business requirement, Adopted industry best practice, Legal Requirement, Contractual Obligation	
A.5.1.2	Review of the policies for information security	The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement, Contractual Requirements	
A.6	**Organization of information Security**						
A.6.1	*Internal Organization*	Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.					
A.6.1.1	Information security roles and responsibilities	All information security responsibilities should be defined and allocated.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement, Contractual Requirements	
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement, Contractual Requirements	
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities should be maintained.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement, Contractual Requirements	
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement, Contractual Requirements	
A.6.1.5	Information security in project management	Information security should be addressed in project management, regardless of the type of the project.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement, Contractual Requirements	
A.6.2	*Mobile devices and teleworking*	Objective: To ensure the security of teleworking and use of mobile devices.					
A.6.2.1	Mobile device policy	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	Y			Business requirement, Adopted industry best practice, Results of Risk Analysis	
A.6.2.2	Teleworking	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	Y			Business requirement, Adopted industry best practice, Results of Risk Analysis	
A.7	**Human resource security**						
A.7.1	*Prior to employment*	Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.					
A.7.1.1	Screening	Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement	
A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement	
A.7.2	*During employment*	Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.					
A.7.2.1	Management responsibilities	Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement	
A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement	
A.7.2.3	Disciplinary process	There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement	
A.7.3	*Termination and change of employment*	Objective: To protect the organization's interests as part of the process of changing or terminating employment.					
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Legal Requirement	
A.8	**Asset management**						
A.8.1	*Responsibility for assets*	Objective: To identify organizational assets and define appropriate protection responsibilities.					
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.8.1.2	Ownership of assets	Assets maintained in the inventory should be owned.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
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 should be identified, documented and implemented.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.8.1.4	Return of assets	All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.8.2	*Information classification*	Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.					
A.8.2.1	Classification of information	Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.8.2.2	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.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.8.2.3	Handling of assets	Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.8.3	*Media handling*	Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.					
A.8.3.1	Management of removable media	Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Y	Y	AWS	Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.8.3.2	Disposal of media	Media should be disposed of securely when no longer required, using formal procedures.	Y	Y	AWS	Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	

INSTRUCTURE		**Statement Of Applicability (ISO 27001:2013)**					

Date: December 13, 2022

ISO 27001 Clause #	Title	Control	Applicability [Y/N]	Controlled by 3rd Party	3rd Party Name	Selection Justification/Exclution - Explanation	Remarks
A.8.3.3	Physical media transfer	Media containing information should be protected against unauthorized access, misuse or corruption during transportation.	Y	Y	AWS	Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9	**Access control**						
A.9.1	*Business requirements of access control*	Objective: To limit access to information and information processing facilities.					
A.9.1.1	Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.1.2	Access to networks and network services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.2	*User access management*	Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.					
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process should be implemented to enable assignment of access rights.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.2.2	User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information should be controlled through a formal management process.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.2.5	Review of user access rights	Asset owners should review users' access rights at regular intervals.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
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 should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.3	*User responsibilities*	Objective: To make users accountable for safeguarding their authentication information.					
A.9.3.1	Use of secret authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.4	*System and application access control*	Objective: To prevent unauthorized access to systems and applications.					
A.9.4.1	Information access restriction	Access to information and application system functions should be restricted in accordance with the access control policy.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.4.3	Password management system	Password management systems should be interactive and should ensure quality passwords.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.9.4.5	Access control to program source code	Access to program source code should be restricted.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.10	**Cryptography**						
A.10.1	*Cryptographic controls*	Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.					
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.11	**Physical and environmental security**						
A.11.1	*Secure areas*	Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.					
A.11.1.1	Physical security perimeter	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.1.2	Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and applied.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.	Y	Y	AWS, Building Facilities	Building facilities manages this requirement, AWS manages the datacenters	
A.11.1.5	Working in secure areas	Procedures for working in secure areas should be designed and applied.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
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 should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Y	Y	AWS, Building Facilities	Building facilities manages this requirement, AWS manages the datacenters	
A.11.2	*Equipment*	Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.					
A.11.2.1	Equipment siting and protection	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.2.2	Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.2.5	Removal of assets	Equipment, information or software should not be taken off-site without prior authorization.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.2.6	Security of equipment and assets off-premises	Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
A.11.2.7	Secure disposal or re-use of equipment	All 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.	Y	Y	TAMS, AWS	TAMS manages local equipment, and AWS manages the datacenters	
A.11.2.8	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.	Y		AWS	Instructure manages the local offices, and AWS manages the datacenters.	
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 should be adopted.	Y		AWS	Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	

INSTRUCTURE		**Statement Of Applicability (ISO 27001:2013)**					

Date: December 13, 2022

ISO 27001 Clause #	Title	Control	Applicability [Y/N]	Controlled by 3rd Party	3rd Party Name	Selection Justification/Exclution - Explanation	Remarks
A.12	**Operation Security**						
A.12.1	*Operational procedure and responsibilities*	Objective: To ensure that security is an integral part of information systems.					
A.12.1.1	Documented operating procedures	Operating procedures should be documented and made available to all users who need them.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.1.3	Capacity management	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.2	*Protection from malware*	Objective: To ensure that information and information processing facilities are protected against malware.					
A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.3	*Backup*	Objective: To protect against loss of data.					
A.12.3.1	Information backup	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.4	*Logging and monitoring*	Objective: To record events and generate evidence.					
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.4.2	Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.4.3	Administrator and operator logs	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.5	*Control of operational software*	Objective: To ensure the integrity of operational systems.					
A.12.5.1	Installation of software on operational systems	Procedures should be implemented to control the installation of software on operational systems.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.6	*Technical Vulnerability Management*	Objective: To prevent exploitation of technical vulnerabilities.					
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users should be established and implemented.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.12.7	*Information systems audit considerations*	Objective: To minimise the impact of audit activities on operational systems.					
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.	Y			Business requirement, Adopted industry best practice	
A.13	**Communications security**						
A.13.1	*Network security management*	Objective: To ensure the protection of information in networks and its supporting information processing facilities.					
A.13.1.1	Network controls	Networks should be managed and controlled to protect information in systems and applications.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.13.1.3	Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.13.2	*Information transfer*	Objective: To maintain the security of information transferred within an organization and with any external entity.					
A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.13.2.2	Agreements on information transfer	Agreements should address the secure transfer of business information between the organization and external parties.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.13.2.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
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 should be identified, regularly reviewed and documented.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.14	**System acquisition, development and maintenance**						
A.14.1	*Security requirements of information systems*	Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.					
A.14.1.1	Information security requirements analysis and specification	The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.1.3	Protecting application services transactions	Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.2	*Security in development and support processes*	Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.					
A.14.2.1	Secure development policy	Rules for the development of software and systems should be established and applied to developments within the organization.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	

ISO 27001 Clause #	Title	Control	Applicability [Y/N]	Controlled by 3rd Party	3rd Party Name	Selection Justification/Exclusion - Explanation	Remarks
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.2.6	Secure development environment	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.2.7	Outsourced development	The organization should supervise and monitor the activity of outsourced system development.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.2.8	System security testing	Testing of security functionality should be carried out during development	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.14.3	**Test data**	Objective: To ensure the protection of data used for testing.					
A.14.3.1	Protection of test data	Test data should be selected carefully, protected and controlled.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements	
A.15	**Compliance**						
A.15.1	**Compliance with legal requirements**	Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.					
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 should be agreed with the supplier and documented.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.15.2	**Supplier service delivery management**	Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.					
A.15.2.1	Monitoring and review of supplier services	Organizations should regularly monitor, review and audit supplier service delivery.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
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, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.16	**Information security incident management**						
A.16.1	**Management of information security incidents and improvements**	Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.					
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.16.1.2	Reporting information security events	Information security events should be reported through appropriate management channels as quickly as possible.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.16.1.4	Assessment of and decision on information security events	Information security events should be assessed and it should be decided if they are to be classified as information security incidents.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.16.1.5	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.16.1.7	Collection of evidence	The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.17	**Information security aspects of business continuity management**						
A.17.1	**Information security continuity**	Objective: Information security continuity should be embedded in the organization's business continuity management systems.					
A.17.1.1	Planning information security continuity	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.17.1.2	Implementing information security continuity	The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.17.1.3	Verify, review and evaluate information security continuity	The organization should 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.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.17.2	**Redundancies**	Objective: To ensure availability of information processing facilities.					
A.17.2.1	Availability of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.18	**Compliance**						
A.18.1	**Compliance with legal and contractual requirements**	Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.					

INSTRUCTURE

Statement Of Applicability
(ISO 27001:2013)

Date: December 13, 2022

ISO 27001 Clause #	Title	Control	Applicability [Y/N]	Controlled by 3rd Party	3rd Party Name	Selection Justification/Exclution - Explanation	Remarks
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 should be explicitly identified, documented and kept up to date for each information system and the organization.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.18.1.2	Intellectual property rights	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.18.1.3	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.	Y			Business requirement, Adopted industry best practice, Data Privacy Requirements, Contractual Requirements, Legal Requirements	
A.18.2	*Information security reviews*	Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.					
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) should be reviewed independently at planned intervals or when significant changes occur.	Y	Y	A-LIGN	Business requirement, Adopted industry best practice	
A.18.2.2	Compliance with security policies and standards	Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Y			Business requirement, Adopted industry best practice	
A.18.2.3	Technical compliance review	Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.	Y			Business requirement, Adopted industry best practice	