a

Statement of Applicability (SoA)

Version date: 3/24/2025

Version 2.0

Introduction

This statement contains an overview of all ISO 27001:2022 Annex A Control Measures, indicating for each control whether it is applicable or not, and whether the control has been implemented in our organization. If a control is excluded, a brief explanation is provided.

Scope description

The scope of our information security management system (ISMS) is:

Information security regarding the development, maintenance and provision of business software in accordance with the Statement of Applicability.

Management measures

No. (ISO 27001:2022)	Description norm requirement	Reason for selection				Applicable? Yes / No	Implemented? Yes / No	Reason for exclusion
		Legislation	Contractual	Best practice	Risk			
A05	**organizational controls**							
A5.1	Policies for information security Information security policies and subject-specific policies shall be defined, approved by management, published, communicated to and recognised by relevant personnel and stakeholders, and reviewed at planned intervals and as significant changes occur.	x		x	x	Y	Y	
A5.2	Information security roles and responsibilities Roles and responsibilities in information security shall be defined and assigned according to the needs of the organization.	x		x	x	Y	Y	
A5.3	Segregation of duties Conflicting duties and conflicting areas of responsibility shall be segregated.	x		x	x	Y	Y	
A5.4	Management responsibilities Management shall require all staff to apply information security in accordance with the organization's adopted information security policy, subject-specific policies and procedures.	x	x	x	x	Y	Y	
A5.5	Contact with authorities The organization shall establish and maintain contact with relevant authorities.	x	x	x	x	Y	Y	
A5.6	Contact with special interest groups The organization shall establish and maintain contacts with special interest groups or other specialised security forums and professional associations.		x	x	x	Y	Y	
A5.7	Threat intelligence Information relating to information security threats shall be collected and analysed to produce threat intelligence.			x	x	Y	Y	
A5.8	Information security in project management Information security shall be integrated into project management.			x	x	Y	Y	
A5.9	Inventory of information and other associated assets An inventory of information and other associated assets, including owners, shall be developed and maintained.			x	x	Y	Y	

A5.10	Acceptable use of information and other associated assets Rules for the acceptable use of and procedures for handling information and other associated assets shall be identified, documented and implemented.		x	x	x	Y	Y	
A5.11	Return of assets Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.		x	x	x	Y	Y	
A5.12	Classification of information Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	x		x	x	Y	Y	
A5.13	Labelling of information An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information clas_x0002_sification scheme adopted by the organization.	x		x	x	Y	Y	
A5.14	Information transfer Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.		x	x	x	Y	Y	
A5.15	Access control Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.		x	x	x	Y	Y	
A5.16	Identity management The full life cycle of identities shall be managed.		x	x	x	Y	Y	
A5.17	Authentication information Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information		x	x	x	Y	Y	
A5.18	Access rights Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.		x	x	x	Y	Y	
A5.19	Information security in supplier relationships Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services	x	x	x	x	Y	Y	
A5.20	Addressing information security within supplier agreements Relevant information security requirements shall be identified and agreed with each supplier based on the type of supplier relationship.			x	x	Y	Y	
A5.21	Managing information security in the information and communication technology (ICT) supply chain Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain			x	x	Y	Y	
A5.22	Monitoring, review and change management of supplier services The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery			x	x	Y	Y	

A5.23	Information security for use of cloud services Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements			x	x	Y	Y	
A5.24	Information security incident management planning and preparation The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.		x	x	x	Y	Y	
A5.25	Assessment and decision on information security events The organization shall assess information security events and decide if they are to be categorized as information security incidents.		x	x	x	Y	Y	
A5.26	Response to information security incidents Information security incidents shall be responded to in accordance with the documented procedures.		x	x	x	Y	Y	
A5.27	Learning from information security incidents Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.		x	x	x	Y	Y	
A5.28	Collection of evidence The organization shall establish and implement procedures for the iden_x0002_tification, collection, acquisition and preservation of evidence related to information security events.		x	x	x	Y	Y	
A5.29	Information security during disruption The organization shall plan how to maintain information security at an appropriate level during disruption.		x	x	x	Y	Y	
A5.30	ICT readiness for business continuity ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.		x	x	x	Y	Y	
A5.31	Legal, statutory, regulatory and contractual requirements Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meeting them shall be identified, documented and kept up to date.	x	x	x	x	Y	Y	
A5.32	Intellectual property rights The organization shall implement appropriate procedures to protect intellectual property rights.	x	x	x	x	Y	Y	
A5.33	Protection of records Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.			x	x	Y	Y	
A5.34	Privacy and protection of personal identifiable information (PII) The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	x	x	x	x	Y	Y	
A5.35	Independent review of information security The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur			x	x	Y	Y	

A5.36	Compliance with policies, rules and standards for information security Compliance with the organization's information security policies, topic-specific policies, rules and standards shall be regularly reviewed.	x		x	x	Y	Y	
A5.37	Documented operating procedures Operating procedures for information processing facilities shall be documented and made available to personnel who need them.			x	x	Y	Y	
A6	**People controls**							
A6.1	Screening Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of			x	x	Y	Y	
A6.2	Terms and conditions of employment The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	x		x	x	Y	Y	
A6.3	Information security awareness, education and training Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.			x	x	Y	Y	
A6.4	Disciplinary process A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.			x	x	Y	Y	
A6.5	Responsibilities after termination or change of employment Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.			x	x	Y	Y	
A6.6	Confidentiality or non-disclosure agreements Confidentiality or non-disclosure agreements reflecting the organ_x0002_ization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	x		x	x	Y	Y	
A6.7	Remote working Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.			x	x	Y	Y	
A6.8	Information security event reporting The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.			x	x	Y	Y	
A7	**Physical controls**							
A7.1	Physical security parameters Security perimeters shall be defined and used to protect areas that contain information and other associated assets.			x	x	Y	Y	
A7.2	Physical access entry Secure areas shall be protected by appropriate entry controls and access points.			x	x	Y	Y	

A7.3	Securing offices, rooms and facilities Physical security for offices, rooms and facilities shall be designed and implemented.			x	x	Y	Y	
A7.4	Physical security monitoring Premises shall be continuously monitored for unauthorized physical access.			x	x	Y	N	
A7.5	Protecting against physical and environmental threats Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.			x	x	Y	Y	
A7.6	Working in secure areas Security measures for working in secure areas shall be designed and implemented.			x	x	Y	Y	
A7.7	Clear desk' and 'clear screen' Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.			x	x	Y	Y	
A7.8	Equipment siting and protection Equipment shall be sited securely and protected.			x	x	Y	Y	
A7.9	Security of assetes off-premises Off-site assets shall be protected			x	x	Y	Y	
A7.10	Storage media Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements,			x	x	Y	Y	
A7.11	Supporting utilities Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.			x	x	Y	Y	
A7.12	Cabling security Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.			x	x	Y	Y	
A7.13	Equipment maintenance Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.			x	x	Y	Y	
A7.14	Secure disposal or re-use of equipment 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.			x	x	Y	Y	
A8	**Technological controls**							
A8.1	'User endpoint devices' Information stored on, processed by or accessed via 'user endpoint devices' shall be protected.			x	x	Y	Y	
A8.2	Privileged access rights The allocation and use of privileged access rights shall be restricted and managed.			x	x	Y	Y	
A8.3	Information access restriction Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.			x	x	Y	Y	
A8.4	Access to source code Read and write access to source code, development tools and software libraries shall be appropriately managed.			x	x	Y	Y	

A8.5	Secure authentication Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.			x	x	Y	Y	
A8.6	Capacity management The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.			x	x	Y	Y	
A8.7	Protection against malware Protection against malware shall be implemented and supported by appropriate user awareness.			x	x	Y	Y	
A8.8	Management of technical vulnerabilities Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.			x	x	Y	Y	
A8.9	Configuration management Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.			x	x	Y	Y	
A8.10	Information deletion Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.			x	x	Y	Y	
A8.11	Data masking Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.			x	x	Y	Y	
A8.12	Data leakage prevention Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information			x	x	Y	Y	
A8.13	Information backup Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.			x	x	Y	Y	
A8.14	Redundancy of information processing facilities Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.			x	x	Y	Y	
A8.15	Logging Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.			x	x	Y	Y	
A8.16	Monitoring activities Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.			x	x	Y	Y	
A8.17	Clock synchronization The clocks of information processing systems used by the organization shall be synchronized to approved time sources.			x	x	Y	Y	

A8.18	Use of privileged utility programs The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.			x	x	Y	Y	
A8.19	Installation of software on operational systems Procedures and measures shall be implemented to securely manage software installation on operational systems.			x	x	Y	Y	
A8.20	Networks security Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.			x	x	Y	Y	
A8.21	Security of network services Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.			x	x	Y	Y	
A8.22	Segregation of networks Groups of information services, users and information systems shall be segregated in the organization's networks.			x	x	Y	Y	
A8.23	Web filtering Access to external websites shall be managed to reduce exposure to malicious content.			x	x	Y	Y	
A8.24	Use of cryptography Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.			x	x	Y	Y	
A8.25	Secure development life cycle Rules for the secure development of software and systems shall be established and applied.			x	x	Y	Y	
A8.26	Application security requirements Information security requirements shall be identified, specified and approved when developing or acquiring applications.			x	x	Y	Y	
A8.27	Secure system architecture and engineering principles Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.			x	x	Y	Y	
A8.28	Secure coding Secure coding principles shall be applied to software development.			x	x	Y	Y	
A8.29	Security testing in development and acceptance Security testing processes shall be defined and implemented in the development life cycle.			x	x	Y	Y	
A8.30	Outsourced development The organization shall direct, monitor and review the activities related to outsourced system development.			x	x	Y	Y	
A8.31	Separation of development, test and production environments Development, testing and production environments shall be separated and secured.		x	x	x	Y	Y	
A8.32	Change management Changes to information processing facilities and information systems shall be subject to change management procedures.			x	x	Y	Y	
A8.33	Test information Test information shall be appropriately selected, protected and managed.			x	x	Y	Y	
A8.34	Protection of information systems during audits Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.			x	x	Y	Y	