SciSure

ISO 27001
Statement of Applicability
ISO/IEC 27001:2022 /Amd.1:2024 - Annex A Controls

The control objectives and measures have been adopted from the ISO/IEC 27001:2022 /Amd.1:2024 standard.

Applicable to: SciSure for Research
Version: 1.2
Date:16/06/2025
Made by: Marijke Koster // Information Security Officer
Approved by: Wouter de Jong // CEO

Control number	Control name	Control description	Applicable yes/no	Implemented yes/no
A. 5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes	Yes
A. 5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes	Yes
A. 5.3	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated.	Yes	Yes
A. 5.4	Management responsibilities	Management shall be a role model for information security and require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes	Yes
A. 5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Yes	Yes
A. 5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	Yes
A. 5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes	Yes
A. 5.8	Information security in project management	Information security shall be integrated into the organization's project management activities.	Yes	Yes
A. 5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes	Yes
A. 5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for the handling of information and other associated assets shall be identified, documented and implemented.	Yes	Yes
A. 5.11	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.	Yes	Yes
A. 5.12	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.	Yes	Yes

Control number	Control name	Control description	Applicable yes/no	Implemented yes/no
A. 5.13	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.	Yes	Yes
A. 5.14	Information transfer	Information transfer rules, procedures, or agreements, both within the organization and between the organization and other parties, shall be in place for all types of transfer facilities.	Yes	Yes
A. 5.15	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.	Yes	Yes
A. 5.16	Identity management	The full life cycle of identities shall be managed.	Yes	Yes
A. 5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel of appropriate handling of authentication information.	Yes	Yes
A. 5.18	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 and rules on access control.	Yes	Yes
A. 5.19	Information security in supplier relationships	Processes and procedures shall be identified and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes	Yes
A. 5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Yes	Yes
A. 5.21	Managing information security in the ICT supply chain	Processes and procedures shall be defined and implemented to address information security risks associated with ICT services and product supply chain.	Yes	Yes
A. 5.22	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.	Yes	Yes
A. 5.23	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.	Yes	Yes
A. 5.24	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.	Yes	Yes

Control number	Control name	Control description	Applicable yes/no	Implemented yes/no
A. 5.25	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.	Yes	Yes
A. 5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Yes
A. 5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the control environment.	Yes	Yes
A. 5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of information from information security incidents.	Yes	Yes
A. 5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes	Yes
A. 5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	Yes
A. 5.31	Identification of legal, statutory, regulatory and contractual requirements	Information security relevant legal, statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes	Yes
A. 5.32	Intellectual property rights	Organizations shall implement appropriate procedures shall be implemented to protect intellectual property rights.	Yes	Yes
A. 5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legal, statutory, regulatory, contractual and business requirements.	Yes	Yes
A. 5.34	Privacy and protection of PII	The organization shall identify and meet the requirements regarding preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	Yes
A. 5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people process and technology shall be reviewed independently at planned intervals, or when significant changes occur.	Yes	Yes
A. 5.36	Compliance with policies and standards for information security	Compliance with the organization's information security policy, topic-specific policies and standards shall be regularly reviewed.	Yes	Yes

Control number	Control name	Control description	Applicable yes/no	Implemented yes/no
A. 5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes	Yes
A. 6	People controls			
A. 6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis in accordance with applicable laws, regulations and ethics, and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Yes
A. 6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes	Yes
A. 6.3	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 organizational policies and procedures, as relevant for their job function.	Yes	Yes
A. 6.4	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.	Yes	Yes
A. 6.5	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.	Yes	Yes
A. 6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	Yes
A. 6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes	Yes
A. 6.8	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.	Yes	Yes

Control number	Control name	Control description	Applicable yes/no	Implemented yes/no
A. 7	People controls			
A. 7.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and other associated assets.	Yes	Yes
A. 7.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls and access points.	Yes	Yes
A. 7.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and implemented.	Yes	Yes
A. 7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Yes	Yes
A. 7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Yes	Yes
A. 7.6	Working in secure areas	Procedures for working in secure areas shall be designed and implemented.	Yes	Yes
A. 7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and enforced.	Yes	Yes
A. 7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Yes	Yes
A. 7.9	Security of assets off-premises	Retrieving data. Wait a few seconds and try to cut or copy again.	Yes	Yes
A. 7.10	Storage media	Storage media shall be managed through its lifecycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	Yes
A. 7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Yes
A. 7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Yes	Yes

Control number	Control name	Control description	Applicable yes/no	Implemented yes/no
A. 7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	Yes
A. 7.14	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.	Yes	Yes
A. 8	Technical controls			
A. 8.1	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and implemented.	Yes	Yes
A. 8.2	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Yes	Yes
A. 8.3	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.	Yes	Yes
A. 8.4	Working in secure areas	Procedures for working in secure areas shall be designed and implemented.	Yes	Yes
A. 8.5	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 enforced.	Yes	Yes
A. 8.6	Equipment siting and protection	Equipment shall be sited securely and protected.	Yes	Yes
A. 8.7	Security of assets off-premises	Retrieving data. Wait a few seconds and try to cut or copy again.	Yes	Yes
A. 8.8	Storage media	Storage media shall be managed through its lifecycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	Yes
A. 8.9	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Yes
A. 8.10	Information deletion	Information stored in information systems and devices shall be deleted when no longer required.	Yes	Yes
A. 8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and business requirement, taking legal requirements into consideration.	Yes	Yes

Control number	Control name	Control description	Applicable yes/no	Implemented yes/no
A. 8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and endpoint devices that process, store or transmit sensitive information.	Yes	Yes
A. 8.13	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.	Yes	Yes
A. 8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Yes
A. 8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, protected, stored and analysed.	Yes	Yes
A. 8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	Yes
A. 8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes	Yes
A. 8.18	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.	Yes	Yes
A. 8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes	Yes
A. 8.20	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Yes	Yes
A. 8.21	Security of network services	Security mechanisms, service levels, and service requirements of network services shall be identified, implemented and monitored.	Yes	Yes
A. 8.22	Segregation in networks	Groups of information services, users, and information systems shall be segregated in the organization's networks.	Yes	Yes
A. 8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Yes	Yes
A. 8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Yes	Yes
A. 8.25	Secure development lifecycle	Rules for the secure development of software and systems shall be established and applied.	Yes	Yes

Control number	Control name	Control description	Applicable yes/no	Implemented yes/no
A. 8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Yes	Yes
A. 8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Yes	Yes
A. 8.28	Secure coding	Secure coding principles shall be applied to software development.	Yes	Yes
A. 8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development lifecycle.	Yes	Yes
A. 8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Yes	Yes
A. 8.31	Separation of development, test and production environments	Development, testing, and production environments shall be separated and secured.	Yes	Yes
A. 8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes	Yes
A. 8.33	Test information	Test information shall be appropriately selected, protected and managed.	Yes	Yes
A. 8.34	Protection of information systems during audit and testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Yes	Yes