Statement of Applicability ISO 27001:2022

Organisation: VamiSec GmbH
Version: 1.0
Approval status: Approved

Template by ICT Institute

For internal use (do not print this part for your official statement of applicability)

Nr.	Chapter	Topic	Control	Applicable to our organisation	Implemented in our organisation	Implementation: How implemented	Implementation: Reference Policy & Procedures	Implementation: Further Evidences for implementation	Implementation: Control owner	Control type	InfoSec properties: Confidentiality	InfoSec properties: Integrity	InfoSec properties: Availability	CyberSec concepts	Operational capabilities	Security domains: Governance and Ecosystem	Security domains: Protection	Security domains: Defence	Security domains: Resilience
				(Yes/No)	(Yes/No)														
5.1	Organizational controls	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	The information security policy and topic-specific guidelines have been defined, approved by management, published, and communicated to relevant employees and interested parties. These policies are reviewed at regular intervals and in the event of significant changes.	Information Security Policy: 2.2. Information Security Policies Document Control Policy: 2.3. Document Approval Process 2.4. Review Cycle of ISMS Documents	Documented Policies: Copies of the approved information security policy and topic-specific policies. Training Materials: Resources to raise employee awareness of the information security policies. Management Presentations: Presentations or reports to management for the approval and review of the policies.	CISO	Preventive	X	X	X	Identify	Governance	X	X		X
5.2	Organizational controls	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes	Yes	The roles and responsibilities in the area of information security are defined and assigned according to the needs of the organization.	Information Security Policy: 4. Roles, Responsibilities, and Authorizations 4.1. Management Team, ISMS Roles and Committees Structure Policy: 2.1 CEO 2.2 Chief Information Security Officer (CISO) 2.3 Information Security Manager (ISM) 2.4 CTO / IT Department 2.5 DPO 2.6 Security Incident Response Lead (SIRT) 2.6.1 Security Operations Center (SOC) 2.7 Vulnerability Manager 2.8 All Employees 2.9 Emergency and Crisis Coordinator 2.10 Risk Owners and Risk Coordinators 2.11 Asset Owner 2.12 Supplier Owner	Organizational charts: Structural diagrams that depict information security roles and responsibilities. Job descriptions: Descriptions of roles that include specific responsibilities for information security. Meeting minutes: Records of meetings in which information security roles and responsibilities were assigned and reviewed.	CISO	Preventive	X	X	X	Identify	Governance	X			X
5.3	Organizational controls	Segregation Of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Yes	Yes	Conflict-prone tasks and areas of responsibility are strictly separated within the organization to avoid conflicts of interest.	Information Security Policy: 4.Roles, Responsibilities, and Authorizations 4.1. Management Team, Information Security Organization Policy and Context 2.1. Understanding the Organization and Its Context 2.3.1. Identifying Interested Parties	Separation of duties: Example processes or workflows that demonstrate the separation of conflict-prone tasks. Audit reports: Results from internal or external audits that confirm proper separation of duties. Training documentation: Training materials that inform staff about the importance and implementation of the separation of duties.	CISO	Preventive	X	X	X	Protect	Governance	X			
5.4	Organizational controls	Management responsibilities	Management shall 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	Management requires all employees to comply with the established information security policy as well as the organization's specific guidelines and procedures.	Information Security Policy: 4.1.Management Team	Communication records: Emails, circulars, or other communication tools sent to staff to ensure compliance with the information security policy. Compliance reports: Reports documenting the degree of compliance by personnel. Management directives: Documented instructions or orders from management to enforce adherence to the security policies.	CEO	Preventive	X	X	X	Identify	Governance	X			
5.5	Organizational controls	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Yes	Yes	The organization has established and continuously maintains contacts with relevant authorities.	Information Security Policy: 2.11. Cooperation with Authorities Incident and IT Emergency Management: 7. Appendix A: Internal Contact Points 8. Appendix B: External Contact Points	Correspondence with authorities: Records or copies of letters and emails between the organization and relevant authorities. Cooperation agreements: Documented agreements or memorandums with authorities for collaboration in the field of information security. Participation records: Meeting minutes or reports from sessions or workshops with authorities	CISO	Preventive Corrective	X	X	X	Protect Respond Recover	Governance			X	X
5.6	Organizational controls	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	The organization establishes and maintains contacts with specialized interest groups, professional forums, and industry associations.	Information Security Policy: 2.7. Awareness, Incident and IT Emergency Management: 8. Appendix B: External Contact Points	Proof of membership: Confirmations of membership in relevant security forums or professional associations. Event documentation: Certificates of participation or minutes from events organized by specialized interest groups or security forums. Collaboration reports: Documented outcomes or reports from cooperation with professional forums and associations.	CISO	Preventive Corrective	X	X	X	Protect Respond Recover	Governance			X	
5.7	Organizational controls	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes	Yes	Information on threats in the area of information security is collected and analyzed to generate threat intelligence.	**Threat intelligence Policy: 3. Threat Intelligence Process 4. Information Sources 5. Integration with the ISMS**	Threat reports: Documented threat analyses and reports. Threat analysis tools: List and functionality of tools used to collect and analyze threat intelligence. Employee training: Training records for staff on threat detection and analysis.	SecOps / IT Ops	Preventive Detective	X	X	X	Identify Detect	Threat_and_ vulnerability_ management		X	X	X
5.8	Organizational controls	Information security in project management	Information security shall be integrated into project management.	Yes	Yes	Information security is systematically integrated into project management.	Information Security Policy: 2.8. Security Requirements in Projects Security in Project Management Policy: 4. Security Integration in Projects	Project Management Policy: Ongoing in another team, must be included and enriched with security aspects. Project plans: Examples of project plans that incorporate information security requirements. Risk assessments: Documented risk assessments for projects related to information security. Audit reports: Reports on the review of projects regarding compliance with security standards.	CISO	Preventive	X	X	X	Identify Protect	Governance	X	X		
5.9	Organizational controls	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes	Yes	An inventory of information and other associated assets, including their owners, is developed and maintained.	Asset Management Policy: 4.3. Method for Creating the Asset Inventory, Risk Management Policy: 4.1.1. Risk Identification Based on Assets	Inventory lists: Current inventories of information and other associated assets. Responsibility assignments: Documents that clarify ownership of specific assets. Audit logs: Reports from audits that verify the accuracy and completeness of the inventory.	CISO	Preventive	X	X	X	Identify	Asset_management	X	X		
5.10	Organizational controls	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Yes	Yes	Rules for acceptable use and procedures for handling information and other associated assets have been identified, documented, and implemented.	Information and Asset Handling Policy: 3. Handling Applications, Systems, and Environments 3.1. General 3.2. Control Systems and System Operations	Acceptable Use Policies: Documented policies for the acceptable use of information resources. Training Programs: Training materials and participation records for courses on handling information and assets. Monitoring Reports: Logs of monitoring activities related to compliance with acceptable use policies.	CISO	Preventive	X	X	X	Protect	Asset_management Information_ protection	X	X		
5.11	Organizational controls	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	Employees and other relevant parties are required to return all assets in the possession of the organization upon change or termination of their employment, contract, or agreement.	Information and Asset Handling Policy: 7. Return of Devices	Return procedures: Documented procedures for returning organizational assets upon termination of contracts. Return logs: Records of asset returns by employees and other relevant parties. Audit reports: Reports from audits verifying compliance with return procedures.	HR Manager	Preventive	X	X	X	Protect	Asset_management		X		
5.12	Organizational controls	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	Information is classified in accordance with the organization's information security requirements, based on confidentiality, integrity, availability, and the needs of relevant interested parties.	Information and Asset Handling Policy: 2.Protection Classes and Handling of Information	Classification schemes: Documents explaining the information classification schemes applied. Training documentation: Materials for training personnel on the classification of information. Monitoring logs: Reports or records monitoring compliance with classification guidelines.	CISO	Preventive	X	X	X	Identify	Information_ protection			X	
5.13	Organizational controls	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Yes	An appropriate set of procedures for labeling information is developed and implemented in accordance with the classification scheme adopted by the organization.	Information and Asset Handling Policy: 2.2.Labeling of Documents	Labeling guidelines: Documented policies and procedures for labeling information. Sample documents: Examples of correctly labeled documents and data. Audit reports: Results of audits confirming compliance with labeling guidelines.	CISO	Preventive	X	X	X	Protect	Information_ protection		X	X	

5,14	Organizational controls	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.	Yes	Yes	Rules, procedures, or agreements for all types of transmission facilities within the organization and between the organization and other parties are in place.	Information and Asset Handling Policy: 3.3. Transmission Technology / Communication	Transfer agreements: Documented agreements for the secure transfer of information. Transfer logs: Records of information transfers. Security measures: Implemented security controls that ensure the secure transfer of information.	CISO	Preventive	X	X	X	Protect	Asset_management Information_ protection		X		
5.15	Organizational controls	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	Rules for controlling physical and logical access to information and other associated assets are established and implemented based on business and information security requirements.	Physical Security Policy: 3.3.4. Protection of Equipment Identity and Access Management Policy: User and Access Administration (2.2), Authentication Methods (3), Privileged Access Management (PAM) (6), Access Controls and Authentication (6.3), Deactivation and Removal of Accounts (7.5), Logging & Monitoring IAM Activities (8), Training & Awareness (9)	Access control policies: Documented policies for physical and logical access to information. Access logs: Records of access requests and approved access rights. Audit reports: Reports from audits that assess the effectiveness of access controls.	CISO	Preventive	X	X	X	Protect	Identity_ and_access_ management		X		
5.16	Organizational controls	Identity management	The full life cycle of identities shall be managed.	Yes	Yes	The complete lifecycle of identities is managed within the organization.	Identity and Access Management Policy: 2. Principles of User and Access Management 4. Integration into HR Processes 5. Regular Review of Roles and Permissions through Recertification 6. Privileged Access Management (PAM)	Identity lifecycle documentation: Documents describing the identity lifecycle from creation to deletion. Access management systems: Logs and reports on identity and access management activities. Audit reports: Reviews of the identity management process by internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	Identity_ and_access_ management		X		
5.17	Organizational controls	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Yes	Yes	The assignment and management of authentication information is controlled through a management process, including staff guidance on the appropriate handling of authentication information.	Identity and Access Management Policy: 3. Authentication Methods 3.1.Password Management 3.2.Multi-Factor Authentication (MFA)	Authentication policies: Documented policies for managing authentication information. Training materials: Resources for training personnel on handling authentication information. Audit logs: Reports on the review of the management and handling of authentication information.	SecOps / IT Ops	Preventive	X	X	X	Protect	Identity_ and_access_ management	X	X		
5.18	Organizational controls	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.	Yes	Yes	Access rights to information and other associated assets are granted, reviewed, modified, and revoked in accordance with the organization's topic-specific access control policy.	Identity and Access Management Policy: 2. Principles of User and Access Management	Access logs: Documented records for the assignment, review, modification, and removal of access rights. Audit reports: Reports on the review of access management by internal or external audits. Training materials: Materials for training staff on managing access rights.	SecOps / IT Ops	Preventive	X	X	X	Protect	Identity_ and_access_ management		X		
5.19	Organizational controls	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.	Yes	Yes	Processes and procedures for managing information security risks related to the use of products or services from suppliers are defined and implemented.	Service Provider and Supplier Management Policy: 4. Requirements for IT Suppliers	PWAG Information Security Code of Conduct for Suppliers and Service Providers Supplier contracts: Documented contracts and agreements with suppliers that include security requirements. Risk assessments: Documented risk analyses related to the use of supplier products or services. Audit reports: Reports on the review of supplier compliance with security requirements.	CISO	Preventive	X	X	X	Identify	Supplier_relationships_ security	X	X		
5.20	Organizational controls	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	Relevant information security requirements are defined and agreed upon with each supplier depending on the type of supplier relationship.	Service Provider and Supplier Management Policy: 4. Requirements for IT Suppliers 4.1. Confidentiality Agreement 4.2. Contractual Security Requirements 4.3.Contract Management 4.4. Basic Security Requirements	Contract documents: Documented security requirements in supplier contracts, Procurement policies: Policies describing how security requirements are included in supplier contracts, Audit reports: Reviews of security requirements in supplier contracts conducted through internal or external audits.	CISO	Preventive	X	X	X	Identify	Supplier_relationships_ security	X	X		
5.21	Organizational controls	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.	Yes	Yes	Processes and procedures for managing information security risks in the supply chain of ICT products and services are defined and implemented.	Service Provider and Supplier Management Policy: 2. Supplier Inventory 2.1. Creation and Maintenance of the Supplier Inventory 2.2. Updating and Review, Asset Management Policy, Risk Management Policy	Supply Chain Risk Management: Documented processes and procedures for managing risks in the ICT supply chain. Supplier assessments: Documented evaluations of the security practices of suppliers in the ICT supply chain. Audit reports: Reports on the review of security management in the ICT supply chain through internal or external audits.	CISO	Preventive	X	X	X	Identify Protect	Supplier_relationships_ security	X	X		
5.22	Organizational controls	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	The organization regularly monitors, reviews, assesses, and manages changes to the information security practices and service delivery of suppliers.	Service Provider and Supplier Management Policy: 4.6. Monitoring and Reporting	Monitoring logs: Regular reports and records on the monitoring and assessment of the information security practices and service delivery of suppliers. Change management logs: Records of the management of changes in supplier services. Audit reports: Reports on the review of supplier management through internal or external audits.	CISO	Preventive	X	X	X	Identify	Supplier_relationships_ security	X	X	X	
5.23	Organizational controls	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	Processes for the acquisition, use, management, and exit of cloud services are established in accordance with the organization's information security requirements.	Use of Cloud Services Policy: 5. Information Security Requirements for IaaS, PaaS, and FaaS Cloud Services	Cloud usage policies: Documented policies and procedures for the secure use of cloud services. Contract documents: Contracts with cloud service providers that include security requirements. Audit reports: Reports on the review of security measures in the use of cloud services.	CISO	Preventive	X	X	X	Protect	Supplier_relationships_ security	X			
5,24	Organizational controls	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	The organization plans and prepares the management of information security incidents by defining, establishing, and communicating processes, roles, and responsibilities in information security incident management.	Incident and IT Emergency Management Policy: 2.4. Activities and Procedures 2.5. Activation, Reaction, and Escalation Times	Incident management plans: Documented plans and procedures for managing information security incidents. Roles and responsibilities: Documents defining the roles and responsibilities within the incident management process. Training documentation: Training records for personnel on handling security incidents.	CISO	Corrective	X	X	X	Respond Recover	Information_security_event_management			X	
5.25	Organizational controls	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	Information security events are assessed by the organization, and a decision is made whether they should be categorized as information security incidents.	Incident and IT Emergency Management Policy: 2.4. Activities and Procedures 2.5. Activation, Reaction, and Escalation Times	Event logs: Records of the assessment of information security events and the decision whether they are classified as incidents. Policies: Documented policies for the assessment of security events. Audit reports: Reports on the review of the incident assessment process through internal or external audits.	CISO	Detective	X	X	X	Detect Respond	Information_security_event_management			X	
5.26	Organizational controls	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Yes	Information security incidents are handled in accordance with documented procedures.	Incident and IT Emergency Management Policy: 2.5.5.Important Points in Incident Handling	Incident response plans: Documented procedures for responding to information security incidents. Incident reports: Records of the response to specific security incidents. Audit reports: Reports on the review of incident response measures through internal or external audits.	SecOps / IT Ops	Corrective	X	X	X	Respond Recover	Information_security_event_management			X	
5.27	Organizational controls	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Yes	Yes	Knowledge gained from information security incidents is used to strengthen and improve information security controls.	Incident and IT Emergency Management Policy: 2.5.6.Follow-Up	Lessons learned reports: Documented insights from the analysis of past information security incidents. Training materials: Materials for training staff on lessons learned from past incidents. Improvement plans: Documented plans to enhance information security measures based on past incidents.	CISO(Supported by: SecOps / IT Ops)	Preventive	X	X	X	Protect Identify	Information_security_event_management			X	
5.28	Organizational controls	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	Yes	The organization establishes and implements procedures for identifying, collecting, recording, and preserving evidence related to information security incidents.	Incident and IT Emergency Management Policy: 2.4.2.Reporting and Recording Events	Evidence handling policies: Documented procedures for the collection, preservation, and retention of evidence related to information security events. Training records: Trainings for employees on handling evidence. Audit reports: Reports on the review of evidence handling processes through internal or external audits.	SecOps / IT Ops	Detective Corrective	X	X	X	Detect Respond	Information_security_event_management		X	X	

5.29	Organizational controls	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes	Yes	The organization plans how to adequately maintain the level of information security during a disruption.	Incident and IT Emergency Management Policy: 3.1.1. IT Emergency (Major Incident) 3.1.2. IT Crisis, Business Continuity Management Policy: 3. Introduction to Business Continuity Management	Continuity plans: Documented plans for maintaining information security during disruptions. Test reports: Records of tests assessing the effectiveness of the plans. Training documentation: Trainings for employees on handling disruptions and maintaining security measures.	CISO	Preventive	X	X	X	Protect	Continuity		X		X
5.30	Organizational controls	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	ICT readiness is planned, implemented, maintained, and tested in accordance with business continuity objectives and ICT continuity requirements.	Incident and IT Emergency Management Policy: 3.3. IT Emergency Management 3.3.1. IT Emergency Team 3.3.2. IT Crisis Team Business Continuity Management Policy: 4.3. Levels of Crisis Situations and Definitions 4.4. Business Continuity and Recovery Planning	ICT contingency plans: Documented plans for ICT readiness in the context of business continuity. Test reports: Records of tests assessing the ICT contingency measures. Audit reports: Reviews of ICT contingency measures through internal or external audits.	CISO	Protective Corrective			X	Protect Respond	Continuity		X		X
5.31	Organizational controls	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes	Yes	Legal, regulatory, contractual, and statutory requirements relevant to information security are identified, documented, and kept up to date.	Information Security Policy: 2.1.2. Regulatory, Legal, and Contractual Compliance, Information Compliance Management Policy: 2. Information Compliance Process: Identifying Requirements, Use of AI Systems Policy: 9. Compliance with AI Requirements	Compliance documents: Current documentation of legal, regulatory, and contractual requirements related to information security. Audit reports: Reports on the review of compliance with legal requirements. Training documentation: Trainings for employees on relevant legal and regulatory requirements.	CISO	Preventive	X	X	X	Identify	Legal_and_ compliance	X			
5.32	Organizational controls	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Yes	Yes	The organization implements appropriate procedures to protect intellectual property rights.	Information Compliance Management Policy: 2.3. Protection of Intellectual Property	IPR protection policies: Documented procedures for the protection of intellectual property. Contracts: Contracts or agreements that include the protection of intellectual property. Audit reports: Reports on the review of measures to protect intellectual property through internal or external audits.	CISO	Preventive	X	X	X	Identify	Legal_and_ compliance	X			
5.33	Organizational controls	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	Yes	Records are protected against loss, destruction, falsification, unauthorized access, and unauthorized disclosure.	Information Compliance Management Policy: 2.4. Protection of Records	Protective measures for records: Documented procedures for protecting records against loss, destruction, or unauthorized access. Audit reports: Reviews of the effectiveness of protective measures through internal or external audits. Backup plans: Plans for the regular backup and archiving of records.	ISM	Preventive	X	X	X	Identify Protect	Legal_and_ compliance Asset_management Information_ protection		X	X	
5.34	Organizational controls	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.	Yes	Yes	The organization identifies and fulfills the requirements related to the protection of personally identifiable information (PII) in accordance with applicable laws, regulations, and contractual obligations.	Information Compliance Management Policy: 2.5. Data Protection, IT Operational Security Policy: 5.4. Test Data Management	Privacy policies: Documented procedures for the protection of PII (personally identifiable information). Compliance reports: Reports on compliance with data protection laws and regulations. Training materials: Training programs for employees on the protection of PII.	DPO	Preventive	X	X	X	Identify Protect	Information_ protection Legal_and_ compliance				
5.35	Organizational controls	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.	Yes	Yes	The organization's approach to information security management and its implementation, including people, processes, and technologies, is independently reviewed at planned intervals or upon significant changes.	Management Review Policy: 5. Management Review Execution 5.1. Agenda and Process	Audit reports: Documented reports of independent reviews of information security measures. Management reviews: Records of management meetings to review information security strategies. External audit reports: Reports from external auditors reviewing the information security measures.	CISO	Preventive Corrective	X	X	X	Identify	Information_security_assurance	X			
###	Organizational controls	Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Yes	Yes	Compliance with the information security policy, topic-specific policies, rules, and standards of the organization is regularly reviewed.	Management Review Policy: 6. Output and Results of the Management Review 6.1. Decisions and Resolutions of Top Management 6.2. New and Updated ISMS Goals	Compliance monitoring reports: Regular reports on the review of compliance with information security policies and standards, Auditor feedback: Feedback from internal and external audits on compliance issues, Training documentation: Evidence of training related to compliance with information security standards.	CISO	Preventive	X	X	X	Protect	Legal_and_ compliance	X	X		
###	Organizational controls	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes	Yes	Operating procedures for information processing facilities are documented and made available to employees who need them.	IT Operational Security: 4. Requirements for Secure IT Operations 4.6. Documentation of IT Operations	Operations documentation: Available and documented operating procedures for information processing systems. Access logs: Records of who can access the operations documentation. Training documentation: Training materials for employees on how to use the operations documentation.	SecOps / IT Ops	Preventive	X	X	X	Protect	Continuity Asset_management Physical_security System_and_network_security	X		X	
6.1	People controls	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 the information to be accessed and the perceived risks.	Yes	Yes	Background checks for all candidates who are to become personnel are conducted prior to joining the organization and on an ongoing basis, considering applicable laws, regulations, and ethical principles, and applied in proportion to business requirements, the classification of information to be accessed, and the perceived risks.	Information Security in HR Processes Policy: 4.2. Hiring 4.2.1. Verification	Screening records: Documented procedures for background checks Audit reports: Reports verifying compliance with screening procedures Training materials: Proof of training for HR staff on the screening procedures.	HR Manager	Preventive	X	X	X	Protect	Human_resource_security	X			
6.2	People controls	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes	Yes	The employment agreements define the responsibilities of personnel and the organization in the area of information security.	Information Security in HR Processes Policy: 4.2.3. Information Security in Employment Contracts	Employment contracts: Documented contracts that clearly define information security responsibilities Compliance reports: Reports reviewing employment contracts for security-related clauses Audit reports: Reports from internal or external audits reviewing the employment contracts.	HR Manager	Preventive	X	X	X	Protect	Human_resource_security	X			
6.3	People controls	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.	Yes	Yes	The organization's personnel and relevant interested parties receive appropriate training and awareness measures on information security, as well as regular updates on the organization's information security policy, topic-specific policies, and procedures relevant to their role.	Information Security in HR Processes Policy: 5.2. Trainings	Training programs: Documented programs and materials for raising awareness and training employees on information security topics Attendance records: Evidence of employee participation in training Feedback mechanisms: Systems for reviewing and improving training programs.	ISM	Preventive	X	X	X	Protect	Human_resource_security	X			
6.4	People controls	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 disciplinary process is formalized and communicated to take action against employees and other relevant interested parties who have violated the information security policy.	Information Security in HR Processes Policy: 5.2. Disciplinary Procedures, Information Security Policy: 2.1.3 Internal Control System	Disciplinary procedures: Documented procedures for disciplinary actions in case of security violations Case studies: Examples of the implementation of disciplinary measures Audit reports: Reports from internal or external audits reviewing the disciplinary procedures.	HR Manager	Preventive Corrective	X	X	X	Protect Respond	Human_resource_security	X			
6.5	People controls	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	Information security responsibilities and obligations that remain valid after termination or change of employment are defined, enforced, and communicated to relevant employees and other interested parties.	Information Security in HR Processes Policy: 7. Leaving the Company	Contract documents: Documented agreements outlining information security responsibilities after the end of employment Communication records: Records of the communication of these responsibilities to personnel Audit reports: Internal or external audit reviews of compliance with post-employment information security responsibilities.	HR Manager	Preventive	X	X	X	Protect	Human_resource_security Asset_management	X			
6.6	People controls	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	Confidentiality or non-disclosure agreements that meet the organization's protection needs are identified, documented, regularly reviewed, and signed by employees and other relevant interested parties.	Information Security in HR Processes Policy: 4.2.3. Information Security in Employment Contracts	Confidentiality agreements: Documented and signed confidentiality or non-disclosure agreements Review records: Regular review and updating of the agreements Training materials: Training programs on the importance and use of confidentiality agreements.	HR Manager	Preventive	X			Protect	Human_resource_security Information_protection Supplier relationships	X	X		
6.7	People controls	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	Security measures are implemented when employees work remotely to protect information that is accessed, processed, or stored outside the organization's premises.	Information and Asset Handling Policy: 4.2. Mobile Working / Teleworking / Mobile Devices Remote Work Policy: Chapter 4.	Remote working policies: Documented security measures for remote work Technical security measures: Records of the implementation of technical security solutions for remote work Audit reports: Reviews of remote work security measures by internal or external audits.	CISO	Preventive	X	X	X	Protect	Asset_management System_and_ network_security Physical_security	X	X		

6.8	People controls	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	The organization provides a mechanism through which personnel can promptly report observed or suspected information security incidents through appropriate channels.	Incident and IT Emergency Management Policy: 2.4.2. Reporting and Recording Events	Reporting protocols: Documented mechanisms for reporting information security incidents Training documentation: Proof of staff training on reporting procedures Audit reports: Reviews of the effectiveness of the reporting procedures by internal or external audits.	SecOps/IT Ops	Detective	X	X	X	Detect	Information_security_event_management		X		
7.1	Physical controls	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	No	No	Not applicable, as VamiSec GmbH operates fully remotely without any owned or managed physical facilities or areas to secure.	Not applicable.	Not applicable. No security perimeters are required or maintained, as the company has no physical office infrastructure.	Not applicable.	Preventive	X	X	X	Protect	Physical_security		X		
7.2	Physical controls	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	No	No	This control is not applicable as the organization operates fully remotely and has no physical secure areas.	Not applicable.	This control is not applicable to VamiSec GmbH, as the organization operates fully remotely and has no physical secure areas.	Not applicable.	Preventive	X	X	X	Protect	Physical_security		X		
7.3	Physical controls	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	No	No	Not applicable due to fully remote operations. Physical security measures apply to home offices and external providers.	Not applicable.	This control is not applicable as the organization operates fully remotely without any physical offices, rooms, or facilities.	Not applicable.	Preventive	X	X	X	Protect	Physical_security Asset_ management		X		
7.4	Physical controls	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	No	No	This control is not applicable, as VamiSec GmbH operates fully remotely without physical secure areas.	Not applicable.	This control is not applicable, as VamiSec GmbH operates fully remotely without physical secure areas.	Not applicable.	Detective	X	X	X	Detect	Physical_security		X		
7.5	Physical controls	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.	No	No	This control is not applicable as the organization operates fully remotely without physical premises.	Not applicable.	This control is not applicable as the organization operates fully remotely without physical premises.	Not applicable.	Preventive	X	X	X	Protect	Physical_security		X		
7.6	Physical controls	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	No	No	Control 7.6 is not applicable as VamiSec GmbH operates fully remotely without physical secure areas. Remote Work Policy in place.	Not applicable.	Control 7.6 is not applicable as VamiSec GmbH operates fully remotely without physical secure areas.	Not applicable.	Preventive	X	X	X	Protect	Physical_security		X		
7.11	Physical controls	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	No	No	Control not applicable due to fully remote operations; protection ensured via cloud provider agreements.	Not applicable.	Control not applicable due to fully remote operations; protection ensured via cloud provider agreements.	Not applicable.	Preventive Detective			X	Protect Detect	Physical_security		X		
7.12	Physical controls	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	No	No	This control is not applicable as VamiSec GmbH operates fully remotely without managing physical cabling infrastructure.	Not applicable.	This control is not applicable as VamiSec GmbH operates fully remotely without managing physical cabling infrastructure.	Not applicable.	Preventive	X		X	Protect	Physical_security		X		
8.1	Technological controls	User endpoint devices	Information stored on, processed by or accessible via user end point devices shall be protected.	Yes	Yes	Information that is stored on, processed through, or accessed via user devices is protected. User endpoint devices are generally protected via Entra ID join, MDM, and EDR. However, a small subset of devices is not currently enrolled in Entra ID or protected by EDR. This gap has been documented and accepted via formal risk acceptance.	IT Operational Security Policy: 11.1. Basic Principles of Client Security; 11.2. Protection Against Malware and Unwanted Applications; 11.3. Data Security and Backup for Clients; 11.5. Mobile Device Management (MDM); 11.6. Monitoring, Anomaly Detection, and Incident Response.	Device Protection Plans: Documented plans for protecting user devices, Monitoring Logs: Records of monitoring the security of user devices, Training Documentation: Training records for staff on the secure handling of user devices	SecOps/IT Ops	Preventive	X	X	X	Protect	Asset_management Information_ protection		X		
8.2	Technological controls	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Yes	Yes	The assignment and use of privileged access rights is restricted and managed.	**Identity and Access Management Policy: 2.1 Principles and Processes, 2.2 User and Access Administration**	Privileged access logs: Records of the allocation and management of privileged access rights, Audit reports: Reports on the review of the management of privileged access rights through internal or external audits, Training documentation: Training records for staff on the management of privileged access rights.	SecOps/IT Ops	Preventive	X	X	X	Protect	Identity_ and_access_ management		X		
8.3	Technological controls	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Yes	Yes	Access to information and other related assets is restricted in accordance with the established topic-specific access control policy.	Identity and Access Management Policy: 2.1 Principles and Processes, 2.2 User and Access Administration	Access policies: Documented policies for access to information and associated assets, Access logs: Records of the monitoring and enforcement of access restrictions, Audit reports: Reports on the review of access restrictions through internal or external audits.	SecOps/IT Ops	Preventive	X	X	X	Protect	Identity_ and_access_ management		X		
8.4	Technological controls	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	No	No	The organization does not currently maintain or develop source code, nor does it use development tools or software libraries in scope. Therefore, access management for source code is not applicable at this time. Procedures are documented and will be activated if software development activities commence.	Not applicable.	VamiSec GmbH does not currently develop or maintain source code, nor use development tools or software libraries within the scope of the ISMS. Therefore, access management for source code is not applicable at this time. Documented procedures for source code access management exist and will be activated if software development activities are initiated.	Not applicable.	Preventive	X	X	X	Protect	Identity_ and_access_ management Application_ security		X		
8.5	Technological controls	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	Yes	Secure authentication technologies and methods are implemented based on access restrictions and the topic-specific access control policy.	**Identity and Access Management Policy: 3.1 Password Management 3.2 Multi-Factor Authentication (MFA)**	Authentication technologies: Documented procedures for the implementation of secure authentication technologies, Training documentation: Training records for staff on the secure use of authentication technologies, Audit reports: Reviews of authentication processes through internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	Identity_ and_access_ management		X		
8.6	Technological controls	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes	Yes	The use of resources is monitored and adjusted in accordance with current and expected capacity requirements. This is achieved using tools such as Intune for Entra ID joined systems. A small number of unmanaged devices are not currently included in centralized capacity monitoring. This limitation has been documented and is covered by a risk acceptance.	IT Operational Security Policy: 3.3. Capacity Management and Prevention of Bottlenecks.	Capacity management plans: Documented plans for monitoring and adjusting resource usage, Monitoring logs: Records of the monitoring of resource usage, Audit reports: Reports on the review of capacity management processes through internal or external audits.	SecOps / IT Ops	Preventive Detective			X	Identify Protect Detect	Continuity	X	X		
8.7	Technological controls	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Yes	Yes	Protective measures against malware are implemented and supported by appropriate user awareness. Most devices are protected via Intune-managed Microsoft Defender for Endpoint. A limited number of unmanaged devices are not enrolled and are covered by a formal risk acceptance. User awareness training applies to all users regardless of device status.	IT Operational Security Policy: 10.3. Protection Against Malware.	Malware protection plans: Documented plans for protection against malware, Monitoring logs: Records of the monitoring and protection against malware, Training documentation: Training records for staff on protection against malware.	SecOps / IT Ops	Preventive Detective Corrective	X	X	X	Protect Detect	System_and_network_security		X	X	
8.8	Technological controls	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.	Yes	Yes	Information about technical vulnerabilities in the information systems in use is gathered primarily through Microsoft Defender for Endpoint. Exposure is evaluated, and appropriate measures are taken. A small subset of devices is not enrolled in Defender and is therefore excluded from automated vulnerability detection. This gap is documented and covered by a formal risk acceptance.	IT Operational Security Policy: 7.1. Identification and Assessment of Vulnerabilities; 7.2. Vulnerability Scans and Penetration Tests; 7.3. Prioritization, Fixing, and Tracking; 7.4. Criticality Levels and Timeframes; 7.5. Monitoring and Reporting; 7.6. Handling Zero-Day Vulnerabilities.	Vulnerability management reports: Documented reports on technical vulnerabilities in information systems, Risk assessments: Documented risk assessments related to technical vulnerabilities, Audit reports: Reports on the review of measures for managing technical vulnerabilities through internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	Threat_and_ vulnerability_ management	X	X	X	
8.9	Technological controls	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes	Yes	Configurations, including security configurations, of hardware, software, services, and networks are created, documented, implemented, monitored, and reviewed.	IT Operational Security Policy: 4.6. Documentation of IT Operations; 5.1. Risk-Based Planning and Approval of Changes; 9.3. Documentation of Administrative Activities.	Configuration management plans: Documented plans for managing configurations, including security configurations, Monitoring logs: Records of the monitoring of configurations, Audit reports: Reports on the review of configuration management processes through internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	Secure_configuration	X	X		
8.10	Technological controls	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Yes	Yes	Information stored in information systems, devices, or other storage media is deleted when it is no longer needed.	IT Operational Security Policy: 4.1. Asset Management, Documentation, Traceability; 4.4. Management of Data Carriers and Media.	Deletion policies: Documented procedures for deleting information in information systems and other storage devices, Audit reports: Reports on the review of compliance with deletion policies through internal or external audits, Training documentation: Training records for staff on the proper deletion of information.	SecOps / IT Ops	Preventive	X			Protect	Information_ protection		X		

8.11	Technological controls	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.	No	No	Data masking is not implemented, as the organization does not use production data for testing or other activities where masking would be required. All development and testing are conducted with synthetic or non-sensitive datasets. Therefore, the control is not applicable in the current environment, and no residual risk has been identified.	IT Operational Security Policy: 5.4. Test Data Management.	Data masking is not implemented, as the organization does not use production data for testing or other activities where masking would be required. All development and testing are conducted with synthetic or non-sensitive datasets. Therefore, the control is not applicable in the current environment, and no residual risk has been identified.	SecOps / IT Ops	Preventive	X			Protect	Information_ protection		X		
8.12	Technological controls	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes	Yes	Measures to prevent data loss are applied to systems, networks, and all other devices that process, store, or transmit sensitive information.	IT Operational Security Policy: 10.3. Protection Against Malware; 10.6. Web Servers. Information and Asset Handling Policy: 2.1. Handling of Protection Classes; 2.2. Labeling of Documents; 3.3. Transmission Technology / Communication: 3.5. Internet; 3.6. Email.	Data leak protection plans: Documented plans for protection against data leaks, Monitoring logs: Records of monitoring and protection against data leaks, Audit reports: Reports on the review of data leak protection measures through internal or external audits.	SecOps / IT Ops	Preventive Detective	X			Protect Detect	Information_ protection		X	X	
8.13	Technological controls	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	Backup and recovery solution is planned using standart Microsoft native services within Azure. Currently partially Implemented. Backup and recovery solution is planned and partially in place using Microsoft Azure native services.Implementation scheduled for 2026. Risk is temporarily accepted until full implementation.	IT Operational Security Policy: 8.1. Backup Concept, Recovery Tests, Emergency Exercises. Data Backup and Recovery Policy: 5. Data Backup Strategy and Planning; 6. Technical and Organizational Measures; 7. Backup Process; 8. Procedures; 9. Testing and Review of Backup Measures.	Design and implement backup and recovery solution based on standart Microsoft Azure native services.	SecOps / IT Ops	Corrective		X	X	Recover	Continuity		X		
8.14	Technological controls	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Yes	Redundancy is partially available through Microsoft Azure architecture (availability zones and failover mechanisms). Risk is temporarily accepted until full solution is in place (scheduled for 2026).	IT Operational Security Policy: 8.1. Backup Concept, Recovery Tests, Emergency Exercises	Risk is temporarily accepted until full implementation.	SecOps / IT Ops	Preventive			X	Protect	Continuity Asset_management		X		X
8.15	Technological controls	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Yes	Yes	Logs that record activities, exceptions, errors, and other relevant events are created, stored, protected, and analyzed for Entra ID joined and managed devices via centralized solutions (e.g., Microsoft Defender and Sentinel). A limited number of unmanaged devices are currently not included in centralized logging. This limitation is documented and covered by an accepted risk.	IT Operational Security Policy: 12.1. Logging Concept and Requirements	Logging policies: Documented procedures for creating, storing, and analyzing logs, Monitoring logs: Records of monitoring and analyzing logs, Audit reports: Reports on the review of logging processes through internal or external audits.	SecOps / IT Ops	Detective	X	X	X	Detect	Information_security_event_management			X	
8.16	Technological controls	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	Yes	Networks, systems, and applications are monitored for anomalous behavior through Microsoft Defender and Sentinel. Monitoring coverage applies to all Entra ID joined systems. A small number of devices are currently excluded from monitoring due to lack of enrollment; this gap is documented and has been accepted as a residual risk.	IT Operational Security Policy: 12.1. Logging Concept and Requirements, 12.2. Monitoring and SIEM, 12.4. Evaluation and Reaction to Anomalies	Monitoring plans: Documented plans for monitoring networks, systems, and applications for anomalous behavior, Monitoring logs: Records of monitoring and responding to anomalous behavior, Audit reports: Reports on the review of monitoring measures through internal or external audits.	SecOps / IT Ops	Detective Corrective	X	X	X	Detect Respond	Information_security_event_management		X	X	
8.17	Technological controls	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes	Yes	The clocks of information processing systems used in the organization are synchronized with approved time sources (Intune or domain-based NTP configuration). A small number of unmanaged devices are not centrally synchronized and are covered by a formal risk acceptance.	IT Operational Security Policy: 10.2. Synchronization of System Time	Time synchronization plans: Documented procedures for synchronizing clocks in information processing systems, Monitoring logs: Records of monitoring and synchronization of clocks, Audit reports: Reports on the review of time synchronization processes through internal or external audits.	SecOps / IT Ops	Detective		X		Protect Detect	Information_security_event_management		X	X	
8.18	Technological controls	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.	Yes	Yes	The use of utility programs that can override system and application controls is restricted and strictly monitored.	IT Operational Security Policy: 9.3. Documentation of Administrative Activities, 9.4. Password Management, PAM	Utility usage policies: Documented procedures for the use of utilities that can override system and application controls, Audit reports: Reports on the review of utility usage through internal or external audits, Training documentation: Training records for staff on the secure handling of utilities.	SecOps / IT Ops	Preventive	X	X	X	Protect	System_and_ network_security Secure_ configuration		X		
8.19	Technological controls	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes	Yes	Procedures and measures for the secure management of software installation on operating systems are implemented. Software deployment and restrictions are centrally managed via Microsoft Intune for Entra ID joined devices. A limited number of unmanaged devices fall outside of this control scope and are covered by a documented risk acceptance.	IT Operational Security Policy: 4.3. Approval Processes for Hardware and Software, 4.5. Operational and Maintenance Times	Installation policies: Documented procedures for the secure installation of software on operating systems, Monitoring logs: Records of monitoring and managing software installations, Audit reports: Reports on the review of installation processes through internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	Secure_configuration		X		
8.20	Technological controls	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Yes	Yes	Networks and network devices are secured, managed, and controlled to protect information in systems and applications. Core infrastructure is protected using firewall rules, VLAN segmentation, and monitoring. Entra ID joined devices are subject to network access control and endpoint protection. A small number of unmanaged devices are not consistently subject to the same controls and are covered by a documented risk acceptance.	IT Operational Security Policy: 10.1. Hardening of Systems, 10.2. Synchronization of System Time	Network security plans: Documented plans for securing and managing networks and network devices, Monitoring logs: Records of monitoring network security, Audit reports: Reports on the review of network security measures through internal or external audits.	SecOps / IT Ops	Preventive Detective	X	X	X	Protect Detect	System_and_network_security		X		
8.21	Technological controls	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Yes	Yes	Security mechanisms, service levels, and service requirements for network services are identified, implemented, and monitored.	IT Operational Security Policy: 10.1. Hardening of Systems, 10.6. Web Servers	Network service security plans: Documented security mechanisms, service levels, and requirements for network services, Monitoring logs: Records of monitoring the security of network services, Audit reports: Reports on the review of security measures for network services through internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	System_and_network_security		X		
8.22	Technological controls	Segregation in networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Yes	Yes	Groups of information services, users, and information systems are separated within the organization's networks.	IT Operational Security Policy: 10.1 Hardening of Systems	Network segmentation plans: Documented procedures for segmenting groups of information services, users, and information systems within the organization's networks, Monitoring logs: Records of monitoring and enforcing network segmentation, Audit reports: Reports on the review of network segmentation measures through internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	System_and_network_security		X		
8.23	Technological controls	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Yes	Yes	Access to external websites is managed to reduce exposure to malicious content using web protection features in Microsoft Defender and browser-based controls on Entra ID joined devices. A small number of unmanaged devices are not currently covered by these controls. This limitation has been documented and accepted as a residual risk.	IT Operational Security Policy: 10.6. Web Servers	Web filtering policies: Documented procedures for managing access to external websites to reduce exposure to malicious content, Monitoring logs: Records of monitoring and enforcing web filtering, Audit reports: Reports on the review of web filtering measures through internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	System_and_network_security		X		
8.24	Technological controls	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Yes	Yes	Rules for the effective use of cryptography, including the management of cryptographic keys, are defined and implemented.	IT Operational Security Policy: 10.4. Cryptography and Key Management	Cryptography policies: Documented procedures for the effective use of cryptography and the management of cryptographic keys, Example documents: Examples of the implementation of cryptographic procedures, Audit reports: Reports on the review of cryptography processes through internal or external audits.	SecOps / IT Ops	Preventive	X	X		Protect	Secure_configuration		X		
8.25	Technological controls	Secure development lifecycle	Rules for the secure development of software and systems shall be established and applied.	No	No	There are currently no in-house or contracted software development activities in scope. Therefore, a secure development lifecycle is not applicable at this time. The organization has prepared a Secure Software Development Policy to be activated when development projects commence.	Not applicable.	There are currently no in-house or contracted software development activities in scope. Therefore, a secure development lifecycle is not applicable at this time. The organization has prepared a Secure Software Development Policy to be activated when development projects commence.	Not applicable.	Preventive	X	X	X	Protect	Application_security System_and_network_security		X		

8.26	Technological controls	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	No	No	Currently, no application development projects are active; therefore, this control is not applicable at this time. The policies and procedures are documented and will be enforced once relevant activities resume.	Not applicable.	Currently, no application development projects are active; therefore, this control is not applicable at this time. The policies and procedures are documented and will be enforced once relevant activities resume.	Not applicable.	Preventive	X	X	X	Protect	Application_security System_and_network_security		X	X	
8.27	Technological controls	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	No	No	The organization currently does not perform or manage system development activities where secure system architecture principles would be applicable. However, relevant principles and documentation are in place and will be applied when development or system engineering projects are initiated.	Not applicable.	The organization currently does not perform or manage system development activities where secure system architecture principles would be applicable. However, relevant principles and documentation are in place and will be applied when development or system engineering projects are initiated.	Not applicable.	Preventive	X	X	X	Protect	Application_security System_and_network_security		X		
8.28	Technological controls	Secure coding	Secure coding principles shall be applied to software development.	No	No	The organization does not currently engage in internal or outsourced software development where secure coding practices would apply. The control is therefore excluded at this time. Secure coding policies and standards are documented and will be enforced when development activities resume.	Not applicable.	The organization does not currently engage in internal or outsourced software development where secure coding practices would apply. The control is therefore excluded at this time. Secure coding policies and standards are documented and will be enforced when development activities resume.	Not applicable.	Preventive	X	X	X	Protect	Application_security System_and_network_security		X		
8.29	Technological controls	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	No	No	The organization does not currently perform software development or system changes requiring security testing as part of a development lifecycle. The control is excluded for the time being. Security testing processes are documented and will be activated once relevant development activities begin.	Not applicable.	The organization does not currently perform software development or system changes requiring security testing as part of a development lifecycle. The control is excluded for the time being. Security testing processes are documented and will be activated once relevant development activities begin.	Not applicable.	Preventive	X	X	X	Detect	Application_security Information_security_assurance System_and_network_security		X		
8.30	Technological controls	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	No	No	Control 8.30 is not applicable as VamiSec GmbH does not outsource any software development activities.	Not applicable.	Control 8.30 is not applicable as VamiSec GmbH does not outsource any software development activities.	Not applicable.	Preventive Detective	X	X	X	Identify Protect Detect	System_and_ network_security Application_security Supplier_relationships_ security	X	X		
8.31	Technological controls	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	No	No	There are currently no development or testing environments in use, as no active software development or system integration projects are ongoing. The control is therefore excluded. Procedures for environment separation are documented and will be implemented when development or test environments are established.	Not applicable.	There are currently no development or testing environments in use, as no active software development or system integration projects are ongoing. The control is therefore excluded. Procedures for environment separation are documented and will be implemented when development or test environments are established.	Not applicable.	Preventive	X	X	X	Protect	Application_security System_and_network_security		X		
8.32	Technological controls	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes	Yes	Changes to information processing facilities and information systems are subject to change management procedures.	IT Operational Security Policy; 5.1. Risk-Based Planning and Approval of Changes Change Management Procedure	Change management policies: Documented procedures for change management in information processing facilities and information systems, Monitoring logs: Records of managing changes, Audit reports: Reports on the review of change management processes through internal or external audits.	SecOps / IT Ops	Preventive	X	X	X	Protect	Application_security System_and_network_security		X		
8.33	Technological controls	Test information	Test information shall be appropriately selected, protected and managed.	No	No	This control is not implemented, as the organization does not conduct system or application testing that involves test information. Consequently, there is no need to select, protect, or manage such information. The control is therefore not applicable in the current context, and no residual risk has been identified.	IT Operational Security Policy; 5.4. Test Data Management	This control is not implemented, as the organization does not conduct system or application testing that involves test information. Consequently, there is no need to select, protect, or manage such information. The control is therefore not applicable in the current context, and no residual risk has been identified.	SecOps / IT Ops	Preventive	X	X		Protect	Information_ protection		X		
8.34	Technological controls	Protection of information systems during audit 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	Audit tests and other assurance activities involving the evaluation of operating systems are planned and coordinated between the auditor and the relevant management.	IT Operational Security Policy; 9.3. Documentation of Administrative Activities	Audit plans: Documented plans for audits and other assurance activities affecting operating systems, Audit reports: Records of planned and conducted audits, Audit agreements: Documented agreements between auditors and management regarding the execution of audit tests.	ISM	Preventive		X	X	Protect	System_and_ network_security Information_protection	X			

Version History				
Version	**Date**	**Changes**	**Author**	**Approver**
0.1	3/3/2025	Creation	Koral Yücel	
1.0	6/10/2025	Review & Final	Koral Yücel	Valeri Milke
Version 1.1	7/29/2025	Added reference to Change Management Procedure (8.32)	Lilia Dorofeeva	Valeri Milke
Version 1.2	8/15/2025	Updated implementation status for controls 8.13 (Information backup) and 8.14 (Redundancy of information processing facilities)	Lilia Dorofeeva	Valeri Milke
Version 1.3	8/20/2025	Updated applicability and implementation notes for controls 8.11 (Data masking) and 8.33 (Test information)	Hilding Karlsson	Valeri Milke

This template was created by the people of ICT Institute

You can find the latest version and other templates here:
https://ictinstitute.nl/free-templates/

You can use this template freely under the Create Commons Attribution license
https://creativecommons.org/licenses/by/4.0/

You can do the following with the templates:

Share. You can share the templates and any documents made with these templates freely, with any one that you want to share it with.
Adapt. You can make new documents based on the templates, make changes, add elements or delete elements as much as you want. You can even do this in commercial organisations of for commercial purposes.

If you are a customer, you do not have to mention ICT Institute anywhere
If you are not a customer, you must keep the text "create by the people of ICT Institute" somewhere

Note that the use of these templates is of course at your own risk.
Note also that the ISO standards are copyrighted. You must buy the standard from NEN or ISO before using it

Read also:
https://ictinstitute.nl/iso-27001-and-nen7510-support/
https://ictinstitute.nl/iso27002-explained-part-1/
https://ictinstitute.nl/iso27002-2022-explained-1/

The SoA is a mandatory ISO27001 document
It contains the set measures from ISO27001:2022's appendix (A5-A8)
The measures are explained in more detail in ISO27002
Further information can be found here:

ICT Institute | ISO27002:2022 explained – Organizational controls
ICT Institute | ISO27002:2022 explained – People controls
ICT Institute | ISO27002:2022 explained – Physical controls
ICT Institute | ISO27002:2022 explained – Technological controls

Value legend:
Yes
No
?
Regulatory compliance
Contractual compliance
Best practice
Risk Analysis

Per control, you should do the following:

Indicate whether it applies to your organization
Give a justification for inclusion. This can be:

Regulatory Compliance	This is mandatory by some applicable law
Contractual compliance	You have agreed with a customer or partner to do this
Best practice	You do it since you think it is useful and others do it as well
Risk analysis	You do it based on a risk from your risk analysis

You should, therefore, first do a risk analysis
and analyse regulatory and contractual requirements before establishing the SoA

If you deem the controls not to apply to your organization, indicate why not (free text)
Next, for the controls that do apply, indicate whether they are actually implemented

The first columns are a mandatory part of the SoA, and should be send to other parties when the SoA is requested.

The final three columns contain internal (confidential) information, and may, therefore, not be shared with outsiders:
How and where the control is implemented
Which organizational role the control owner (responsible person) is
Whether there is a regular check on the contol. Regular checks and evaluations are mandatory in an ISO27001 compliant ISMS.

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
NOTE 1 Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;
NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.
NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

d) produce a Statement of Applicability that contains:
— the necessary controls (see 6.1.3 b) and c));
— justification for their inclusion;
— whether the necessary controls are implemented or not; and
— the justification for excluding any of the Annex A controls.

e) formulate an information security risk treatment plan; and

f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.
NOTE 4 The information security risk assessment and treatment process in this document aligns with the principles and generic guidelines provided in ISO 31000[5].