IMPLEMENTING SECURITY CONTROLS

INTRODUCTION TO ANNEX A OF ISO 27001:2022 - CONTROLS AND OBJECTIVES

ISO 27001 security controls are structured as follows:

- Organizational controls
- People controls
- Physical controls
- Technological controls

5	Organizational controls	
5.1	Policies for information Security	**Control** 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.
5.2	Information security roles and responsibilities	**Control** Information security roles and responsibilities shall be defined andallocated according to the organization's needs.
5.3	Segregation of duties	**Control** Conflicting duties and conflicting areas of responsibility shall be segregated.
5.4	Management responsibilities	**Control** 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.
5.5	Contact with authorities	**Control** The organization shall establish and maintain contact with relevant authorities.
5.6	Contact with special interest groups	**Control** The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
5.7	Threat intelligence	**Control** Information relating to information security threats shall be collectedand analyzed to produce threat intelligence.
5.8	Information security in projectmanagement	**Control** Information security shall be integrated into project management.
5.9	Inventory of information andother associated assets	**Control** An inventory of information and other associated assets,

		includingowners, shall be developed and maintained.
5.10	Acceptable use of informationand other associated assets	**Control** Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented, and implemented.
5.11	Return of assets	**Control** 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.
5.12	Classification of information	**Control** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.
5.13	Labeling of information	**Control** An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
5.14	Information transfer	**Control** Information transfer rules, procedures, or agreements shall be in placefor all types of transfer facilities within the organization and between the organization and other parties.
5.15	Access control	**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.
5.16	Identity management	**Control** The full life cycle of identities shall be managed.
5.17	Authentication information	**Control** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on the appropriate handling of authentication information.
5.18	Access rights	**Control** 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.
5.19	Information security in supplierrelationships	**Control** Processes and procedures shall be defined and implemented to managethe information security risks associated with the use of the supplier's products or services.
5.20	Addressing information securitywithin supplier agreements	**Control** Relevant information security requirements shall be established andagreed upon with each supplier based on the type of supplier relationship.
5.21	Managing information security in the information and communication technology (ICT) supply chain	**Control** Processes and procedures shall be defined and implemented to managethe information security risks associated with the ICT products and services supply chain.
5.22	Monitoring, reviewing, and changemanagement of supplier services	**Control** The organization shall regularly monitor, review, evaluate, and manage changes in supplier information security practices and service delivery.
5.23	Information security for the use of cloud services	**Control** Processes for acquisition, use, management, and exit from cloud services shall be established in accordance with the organization's information security requirements.
5.24	Information security incident management planning and preparation	**Control** The organization shall plan and prepare for managing information security incidents by defining, establishing, and communicating informationsecurity incident management processes, roles, and responsibilities.
5.12	Classification of information	**Control** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.
5.13	Labeling of information	**Control** An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
5.14	Information transfer	**Control** Information transfer rules, procedures, or agreements shall be in placefor all types of transfer facilities within the

		organization and between the organization and other parties.
5.15	Access control	**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.
5.16	Identity management	**Control** The full life cycle of identities shall be managed.
5.17	Authentication information	**Control** Allocation and management of authentication information shall be controlled by a management process, including advising personnel on the appropriate handling of authentication information.
5.18	Access rights	**Control** 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.
5.19	Information security in supplierrelationships	**Control** Processes and procedures shall be defined and implemented to managethe information security risks associated with the use of the supplier's products or services.
5.20	Addressing information securitywithin supplier agreements	**Control** Relevant information security requirements shall be established andagreed upon with each supplier based on the type of supplier relationship.
5.21	Managing information security in the information and communication technology (ICT) supply chain	**Control** Processes and procedures shall be defined and implemented to managethe information security risks associated with the ICT products and services supply chain.
5.22	Monitoring, review, and changemanagement of supplier services	**Control** The organization shall regularly monitor, review, evaluate, and manage changes in supplier information security practices and service delivery.
5.23	Information security for the use of cloud services	**Control** Processes for acquisition, use, management, and exit from cloud services shall be established in accordance with the organization's information security requirements.

5.24	Information security incident management planning and preparation	**Control** The organization shall plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles, and responsibilities.
5.25	Assessment and decision on information security events	**Control** The organization shall assess information security events and decide if they are to be categorized as information security incidents.
5.26	Response to information security incidents	**Control** Information security incidents shall be responded to in accordance with the documented procedures.
5.27	Learning from information se-security incidents	**Control** Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.
5.28	Collection of evidence	**Control** The organization shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.
5.29	Information security during disruption	**Control** The organization shall plan how to maintain information security at an appropriate level during disruption.
5.30	ICT readiness for business continuity	**Control** ICT readiness shall be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.
5.31	Legal, statutory, regulatory, and contractual requirements	**Control** 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.
5.32	Intellectual property rights	**Control** The organization shall implement appropriate procedures to protect intellectual property rights.
5.33	Protection of records	**Control** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

5.34	Privacy and protection of personally identifiable information (PII)	**Control** 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.
5.35	Independent review of information security	**Control** 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.
5.36	Compliance with policies, rules, and standards for information security	**Control** Compliance with the organization's information security policy, topic-specific policies, rules, and standards shall be regularly reviewed.
5.37	Documented operating procedures	**Control** Operating procedures for information processing facilities shall be documented and made available to personnel who need them.
6	**People controls**	
6.1	Screening	**Control** 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.
6.2	Terms and conditions of employment	**Control** The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.
6.3	Information security awareness, education, and training	**Control** 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.
6.4	Disciplinary process	**Control** A disciplinary process shall be formalized and communicated to

		take action against personnel and other relevant interested parties who have committed an information security policy violation.
6.5	Responsibilities after termination or change of employment	**Control** 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.
6.6	Confidentiality or non-disclosure agreements	**Control** 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.
6.7	Remote working	**Control** Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.
6.8	Information security event reporting	**Control** The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.
7	**Physical controls**	
7.1	Physical security perimeters	**Control** Security perimeters shall be defined and used to protect areas that contain information and other associated assets.
7.2	Physical entry	**Control** Secure areas shall be protected by appropriate entry controls and access points.
7.3	Securing offices, rooms and facilities	**Control** Physical security for offices, rooms, and facilities shall be designed and implemented.

7.4	Physical security monitoring	**Control** Premises shall be continuously monitored for unauthorized physical access.
7.5	Protecting against physical and environmental threats	**Control** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.
7.6	Working in secure areas	**Control** Security measures for working in secure areas shall be designed and implemented.
7.7	Clear desk and clear screen	**Control** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
7.8	Equipment siting and protection	**Control** Equipment shall be sited securely and protected.
7.9	Security of assets off-premises	**Control** Off-site assets shall be protected.
7.10	Storage media	**Control** Storage media shall be managed through their life cycle of acquisition, use, transportation, and disposal in accordance with the organization's classification scheme and handling requirements.
7.11	Supporting utilities	**Control** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.
7.12	Cabling security	**Control** Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.
7.13	Equipment maintenance	**Control** Equipment shall be maintained correctly to ensure the availability, integrity and confidentiality of information.
7.14	Secure disposal or re-use of equipment	**Control** Items of equipment containing storage media shall be verified

		to ensure that any sensitive data and licensed software has been removedor securely overwritten prior to disposal or re-use.
8	**Technological controls**	
8.1	User endpoint devices	**Control** Information stored on, processed by, or accessible via user end-pointdevices shall be protected.
8.2	Privileged access rights	**Control** The allocation and use of privileged access rights shall be restrictedand managed.
8.3	Information access restriction	**Control** Access to information and other associated assets shall be restricted inaccordance with the established topic-specific policy on access control.
8.4	Access to source code	**Control** Read and write access to source code, development tools, and softwarelibraries shall be appropriately managed.
8.5	Secure authentication	**Control** Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.
8.6	Capacity management	**Control** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
8.7	Protection against malware	**Control** Protection against malware shall be implemented and supported byappropriate user awareness.
8.8	Management of technical vulnerabilities	**Control** 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.
8.9	Configuration management	**Control** Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented,monitored and reviewed.
8.10	Information deletion	**Control** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.

8.11	Data masking	**Control** 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.
8.12	Data leakage prevention	**Control** Data leakage prevention measures shall be applied to systems, networks, and any other devices that process, store or transmit sensitive information.
8.13	Information backup	**Control** Backup copies of information, software, and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policyon backup.
8.14	Redundancy of information processing facilities	**Control** Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
8.15	Logging	**Control** Logs that record activities, exceptions, faults, and other relevant eventsshall be produced, stored, protected, and analyzed.
8.16	Monitoring activities	**Control** Networks, systems, and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.
8.17	Clock synchronization	**Control** The clocks of information processing systems used by the organizationshall be synchronized to approved time sources.
8.18	Use of privileged utility programs	**Control** The use of utility programs that can be capable of overriding systemand application controls shall be restricted and tightly controlled.
8.19	Installation of software on operational systems	**Control** Procedures and measures shall be implemented to securely managesoftware installation on operational systems.
8.20	Networks security	**Control** Networks and network devices shall be secured, managed, and controlled to protect information in systems and applications.
8.21	Security of network services	**Control** Security mechanisms, service levels, and service requirements of network services shall be identified, implemented, and monitored.

8.22	Segregation of networks	**Control** Groups of information services, users and information systems shallbe segregated in the organization's networks.
8.23	Web filtering	**Control** Access to external websites shall be managed to reduce exposure tomalicious content.
8.24	Use of cryptography	**Control** Rules for the effective use of cryptography, including cryptographic keymanagement, shall be defined and implemented.
8.25	Secure development life cycle	**Control** Rules for the secure development of software and systems shall be established and applied.
8.26	Application security requirements	**Control** Information security requirements shall be identified, specified, and approved when developing or acquiring applications.
8.27	Secure system architecture and engineering principles	**Control** Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system development activities.
8.28	Secure coding	**Control** Secure coding principles shall be applied to software development.
8.29	Security testing in developmentand acceptance	**Control** Security testing processes shall be defined and implemented in thedevelopment life cycle.
8.30	Outsourced development	**Control** The organization shall direct, monitor, and review the activities relatedto outsourced system development.
8.31	Separation of development, testand production environments	**Control** Development, testing, and production environments shall be separatedand secured.
8.32	Change management	**Control** Changes to information processing facilities and information systemsshall be subject to change management procedures.
8.33	Test information	**Control** Test information shall be appropriately selected, protected and managed.

8.34	Protection of information systems during audit testing	**Control** Audit tests and other assurance activities involving the assessment of operational systems shall be planned and agreed upon between the tester and appropriate management.