ISO/IEC 27001:2022 controls used in context of Clause *6.1.3 Information security risk treatment*

A.5	Organizational controls	
A.5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.
A.5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.
A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated
A.5.4	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
A.5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities
A.5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
A.5.7	Threat Intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.
A.5.8	Information security in project management	Information security shall be integrated into project management
A.5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.
A.5.10	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.
A.5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.
A.5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements
A.5.13	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.
A.5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties
A.5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.
A.5.16	Identity Management	The full life cycle of identities shall be managed.
A.5.17	Authentication Information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.
A.5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.
A.5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.
A.5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
A.5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
A.5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
A.5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.
A.5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.
A.5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.
A.5.26	Response to Information security incidents	Information security incidents shall be responded to in accordance with the documented procedures
A.5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.
A.5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.