ISO 27001:2022

AUDIT CHECKLIST

PART 2

A.5 ORGANISATION CONTROLS

MINISTRY OF SECURITY

A.5 Operational Controls				
Control No.	**Control**	**Control Description**	**Gap Assessment Questions**	**Response**
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.	1. Do Security policies exist. 2. Are all policies approved by management. 3. Are policies properly communicated to employees. 4. Are security policies subject to review. 5. Are the reviews conducted at regular intervals. 6. Are reviews conducted when circumstances change.	
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	1. Are the employees properly briefed on their information security roles and responsibilities prior to being granted access to the organization's information and other associated assets. 2. Are responsibilities for the protection of individual assets and Responsibilities for information security risk management activities and in particular for acceptance of residual risks should be defined.	
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	1. Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services.	
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.	1. Does the management demonstrate support of the information security policy, topic-specific policies, procedures and information security controls. 2. Does the management ensures that personnel achieve a level of awareness of information security relevant to their roles and responsibilities within the organization. 3. Does the management ensures that personnel are provided with adequate resources and project planning time for implementing the organization's security-related processes and controls.	
5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	"1. Is there a procedure documenting when, and by whom, contact with relevant authorities (law enforcement etc.) will be made. 2. Is there a process, which details how and when contact, is required? 3. Is there a process for routine contact and intelligence sharing.	
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.	1. Do relevant individuals within the organisation maintain active membership in relevant special interest groups. 2. Does relevant individuals within the organization gain knowledge about best practices and stay up to date with relevant security information. 3. Does relevant individuals within the organization share and exchange information about new technologies, products, services, threats or vulnerabilities.	

5.7	Threat intelligence	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	1. Is there a documented policy/procedure describing process for collecting, analyzing and evaluating information related to information security threats. 2. Does the threat intelligence program ensure that the information collected related to information security threats are relevant, insightful, contextual and actionable. 3. Does the threat intelligence program has a formal process for identifying, vetting and selecting internal and external information security threat sources and analyzing information to understand the impact to the organization.	
5.8	Information security in project management	Information security shall be integrated into project management.	1. Is there a documented policy/procedure describing process to ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle. 2. Are the information security risks assessed and treated at an early stage and periodically as part of project risks throughout the project life cycle. 3. Are the requirements regards to compliance with the legal, statutory, regulatory and contractual requirements considered throughout the project management life cycle?	
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	1. Is there an inventory of all assets associated with information and information processing facilities. 2. Is the inventory accurate and kept up to date. 3. Are the asset owners identified and tagged to all assets. 4. Is the asset inventory updated when assets are procured, decommissioned or disposed.	
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.	1. Is there a documented policy/procedure describing process to ensure information and other associated assets are appropriately protected, used and handled. 2. Is the policy approved by the management. 3. Is the policy communicated to all individuals of the organization. 4. Does the policy at minimum covers expected and unacceptable behaviors of employees from an information security perspective.	
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.	1. Is there a process in place to ensure all employees and external users return the organisation's assets on termination of their employment, contract or agreement. 2. Is the organization following the defined process for collecting all physical and electronic assets provided to the employee.	

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.	1. Is there a documented policy/procedure describing process to classify information and assets based on the criticality and sensitivity of the information. 2. Are the requirements for confidentiality, integrity and availability considered for the classification. 3. Is the classification scheme defined and followed for information classification. 4. Are the information owners involved in classifying the information under their control. 5. Is there a defined process for declassifying or to change the classification of the information. 6. Is the information classification reviewed on periodic basis.	
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.	1. Is there a documented policy/procedure describing process to label the information within the organization. 2. Does the labelling process defined the contents to be included in the label.	
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.	1. Is there a documented policy/procedure describing process to maintain the security of information transferred within an organization and with any external interested parties. 2. Are procedures for how data should be transferred made available to all employees. 3. Are relevant technical controls in place to prevent non-authorised forms of data transfer 4.Is there a documented policy and process detailing how physical media should be transported. 5. Is media in transport protected against unauthorised access, misuse or corruption.	
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.	1. Is there a documented policy/procedure describing process to manage logical and physical access to information, assets and information processing assets. 2. Is the policy based on business requirements. 3. Is the policy communicated appropriately. 4. Does the access management include the principles of "need-to-know" and "need-to-use" for managing logical and physical access to information, assets and information processing facilities.	
5.16	Identity management	The full life cycle of identities shall be managed.	1. Are the employees provided with unique IDs for accessing information, assets and information processing facilities. 2. Shared user IDs/Accounts are only authorized when necessary for business purposes and after approvals 3. Are the Identities removed/disabled when no longer needed.	

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.	1. Is there a documented policy/procedure describing process to distribute or assign authentication credentials for employees. 2. Is there a documented policy/procedure describing the baseline requirements of authentication credentials(passwords/passphrases/PINs) used for accessing organization information, assets and information processing facilities. 2. Are the passwords/authentication credentials communicated to employees via a secured channel. 3. Are the employees prompted to change the credentials upon first login. 4. Is there a formal process for resetting authentication credentials.	
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.	1. Are the assess rights assigned considering the business requirements and individual's roles and responsibilities. 2. Is the principle of segregation of duties considered while provisioning access rights. 3. are appropriate approvals taken from asset/information owners for provisioning or revoking access rights. 4. Is there a predefined frequency for reviewing the access rights. 5. Are the access rights modified upon change of job role or termination.	
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.	1. Is there a documented policy/procedure describing process to manage information security risks associated with the use of supplier's products or services. 2. Are the vendors/suppliers evaluated with the organization's requirements for information security. 3. Are the process defined for handling incidents and contingencies associated with supplier products and services. 4. Are suppliers/vendors provided with documented security requirements? 5. Is supplier/vendor's access to information assets & infrastructure controlled and monitored?	
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.	1. Are the information security requirements included in contracts established with suppliers and service providers? 2. Does the contracts established with supplier and service providers include legal, statutory, regulatory, data protection, handling of personally identifiable information (PII), intellectual property rights and copyright requirements. 3. Does the contracts established with supplier and service providers include rules of acceptable use of organization's information and information assets.	
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.	1. Do supplier agreements include requirements to address information security within the service & product supply chain.	

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.	1. Is there a documented policy/procedure describing process to maintain an agreed level of information security and service delivery in line with supplier agreements. 2. Are the SLA's (Service Level Agreements) defined for all service providers . 3. Are there any periodic checks done to ensure the supplier is delivering the agreed level of services to the organization.	
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.	1. Is there a documented policy/procedure describing process to manage information security for the use of cloud services within the organization. 2. Are the roles and responsibilities related to the use and management of cloud services defined. 3. Is there a process defined to o obtain assurance on information security controls implemented by cloud service providers. 4. Is there a process defined for handling information security incidents that occur in relation to the use of cloud services.	
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.	1. Is there a documented policy/procedure describing process for quick, effective, consistent and orderly response to information security incidents. 2. Is there a process for reporting of identified information security weaknesses. 3. Is this process communicated to all employees and interested parties as applicable 4. Are the members of incident management team provided with appropriate training for managing incidents. 5. Is the incident response plan tested on periodic basis.	
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.	1. Is there a process to ensure information security events are properly assessed and classified. 2. Is there a process to categorize and prioritise incidents based on the impact.	
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	1. Is there a process defined for responding to information security incidents. 2. Is there documented response timelines for all categories of incidents. 3. Is there a process to understand and analyse the root cause for the incidents. 4. Are the actions taken to mitigate the incident effective .	
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	1. Is there a process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events. 2. Is there a process to enhance the incident management plan including incident scenarios and procedures from the learnings.	

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.	1. Is there a process in place to ensure a consistent and effective management of evidence related to information security incidents. 2. In the event of an information security incident is relevant data collected in a manner which allows it to be used as evidence.	
5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	1. Is there a documented policy/procedure describing process to protect information and other associated assets during disruption. 2. Is there a process to maintain existing information security controls during disruption.	
5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	1. Is there a documented policy/procedure to ensure the availability of the organization's information and other associated assets during disruption. 2. Is information security included in the organisation's continuity plans. 3. Do information processing facilities have sufficient redundancy to meet the organisations availability requirements. 4. Does the organization test its continuity plan on a periodic basis.	
5.31	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.	1. Is there a process in place to ensure compliance with legal, statutory, regulatory and contractual requirements related to information security. 2. Are the responsibilities assigned to individuals for managing legal, statutory, regulatory and contractual requirements related to information security. 3. Are the actions taken to meet legal, statutory, regulatory and contractual requirements related to information security reviewed to check their effectiveness.	
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	1. Does the organisation keep a record of all intellectual property rights and use of proprietary software products. 2. Does the organisation monitor for the use of unlicensed software. 3. Are processes in place for acquiring software only through known and reputable sources, to ensure that copyright is not violated. 4. Are processes in place to ensure that any maximum number of users permitted within the license is not exceeded.	
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	1. Are records protected from loss, destruction, falsification and unauthorized access or release in accordance with legislative, regulatory, contractual and business requirements. 2. Are controls on place for storage, handling chain of custody and disposal of records.	
5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	1. Is there a process in place to ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII. 2. Is the process communicated to all relevant interested parties involved in the processing of personally identifiable information.	

5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	1. Is there a process in place to ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security. 2. Is the organisations approach to managing information security subject to regular independent review? 3. Is the implementation of security controls subject to regular independent review.	
5.36	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.	1. Is there a process in place to ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards. 2. If a non compliance is identified is there a process to identify the causes of the non-compliance, implementing corrective actions and reviewing the actions taken to evaluate the effectiveness.	
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	1. Are operating procedures well documented. 2. Are the procedures made available to all users who need them. 3. Does the operating procedures specify responsibilities of individuals.	

FOLLOWED BY PART 3: A.6 - PEOPLE CONTROLS & A.7 - PHYSICAL CONTROLS

FOLLOW US ON LINKEDIN FOR MORE FREE CHECKLISTS

PLAYBOOK MADE WITH ❤ MINISTRY OF SECURITY