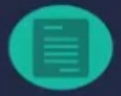
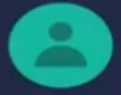
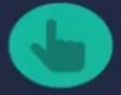
ISO27001:2022
Lec6

Annex A

The 14 Domains of ISO 27001


Information Security Policies


Human Resource Security


Access Control


Physical and Environmental Security


Operations Security


Organization of Information Security

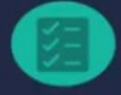

Asset Management

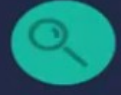

Cryptography

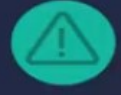

System Acquisition, Development, and Maintenance


Supplier Relationships


Communication Security


Business Continuity Management


Compliance


Information Security Incident Management

A.5 - Information Security Policies

A.5 Information security policies

A.5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 Policies for information security

Control

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

A.5.1.2 Review of the policies for information security

Control

The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

A.6 – Organization of Information Security

A.6 Organization of information security

A.6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A.6.1.1 Information security roles and responsibilities

Control

All information security responsibilities shall be defined and allocated.

A.6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

A.6 – Organization of Information Security

A.6 Organization of information security

A.6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A.6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities shall be maintained.

A.6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6.1.5 Information security in project management

Control

Information security shall be addressed in project management, regardless of the type of the project.

A.6 – Organization of Information Security

A.6 Organization of information security

A.6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

A.6.2.1 Mobile device policy

Control

A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

A.6.2.2 Teleworking

Control

A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

A.6 Organization of information security

A.6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

A.6.2.1 Mobile device policy

Control

A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

A.6.2.2 Teleworking

Control

A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

A.7 - Human Resources Security

A.7 Human resource security

A.7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suit-able for the roles for which they are considered.

A.7.1.1 Screening

Control

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

A.7.1.2 Terms and conditions of employment

Control

The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

A.7 - Human Resources Security

A.7 Human resource security

A.7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

A.7.2.1 Management responsibilities

Control

Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

A.7.2.2 Information security awareness, education and training

Control

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

A.7 - Human Resources Security

A.7.2.3 Disciplinary process

Control

There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

A.7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

A.7.3.1 Termination or change of employment responsibilities

Control

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

A.8 – Asset Management

A.8 Asset management

A.8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

A.8.1.1 Inventory of assets

Control

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

A.8.1.2 Ownership of assets

Control

Assets maintained in the inventory shall be owned.

A.8 – Asset Management

A.8 Asset management

A.8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

A.8.1.3 Acceptable use of assets

Control

Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

A.8.1.4 Return of assets

Control

All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

A.8 – Asset Management

A.8 Asset management

A.8.2 Information classification

Objective: Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

A.8.2.1 Classification of information

Control

Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

A.8.2.2 Labelling of information

Control

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.8 – Asset Management

A.8 Asset management

A.8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

A.8.3.1 Management of removable media

Control

Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

A.8.3.2 Disposal of media

Control

Media shall be disposed of securely when no longer required, using formal procedures.

A.8.3.3 Physical media transfer

Control

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

A.9 – Access Control

A.9 Access control

A.9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

A.9.1.1 Access control policy

Control

An access control policy shall be established, documented and reviewed based on business and information security requirements.

A.9.1.2 Access to networks and network services

Control

Users shall only be provided with access to the network and net- work services that they have been specifically authorized to use.

A.9 – Access Control

A.9 Access control

A.9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

A.9.2.1 User registration and de-registration

Control

A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

A.9.2.2 User access provisioning

Control

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

A.9 – Access Control

A.9 Access control

A.9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

A.9.2.5 Review of user access rights

Control

Asset owners shall review users' access rights at regular intervals.

A.9.2.6 Removal or adjustment of access rights

Control

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9 – Access Control

A.9 Access control

A.9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

A.9.3.1 Use of secret authentication information

Control

Users shall be required to follow the organization's practices in the use of secret authentication information.

A.9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

A.9.4.1 Information access restriction

Control

Access to information and application system functions shall be restricted in accordance with the access control policy.

A.9 – Access Control

A.9 Access control

A.9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

A.9.4.2 Secure log-on procedures

Control

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

A.9.4.3 Password management system

Control

Password management systems shall be interactive and shall ensure quality passwords.

A.9 – Access Control

A.9 Access control

A.9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

A.9.4.4 Use of privileged utility programs

Control

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

A.9.4.5 Access control to program source code

Control

Access to program source code shall be restricted.

A.9 – Cryptography

A.10 Cryptography

A.10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1 Policy on the use of cryptographic controls

Control

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

A.10.1.2 Key management

Control

A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

A.9 –Cryptographic Controls Standard

A. **Confidentiality**: using encryption of information to protect against unauthorized access to information, either stored or transmitted.

B. **Integrity/Authenticity**: using message authentication codes or digital signatures to protect the authenticity and integrity of stored or transmitted information.

C. **Non-repudiation**: using cryptographic techniques to assist with determining proof of the occurrence or non-occurrence of an event.

D. **Authentication**: e.g. certificate Authority (CA) based authentication.

A.9 – Cryptography

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

THANKS!