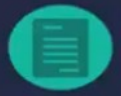
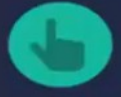
Annex A – Continued

The 14 Domains of ISO 27001



Information Security Policies

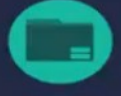
Human Resource Security



Access Control

Physical and Environmental Security

Operations Security

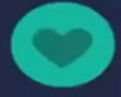


Organization of Information Security

Asset Management

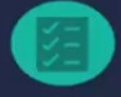
Cryptography

System Acquisition, Development, and Maintenance



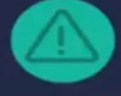
Supplier Relationships

Communication Security



Business Continuity Management

Compliance



Information Security Incident Management

A.14 – System Acquisition, Development and Maintenance

A.14 System acquisition, development and maintenance

A.14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A.14.1.1 Information security requirements analysis and specification

Control

The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

A.14.1.2 Securing application services on public networks

Control

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

A.14 – System Acquisition, Development and Maintenance

A.14.1.3 Protecting application services transactions

Control

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

A.14 – System Acquisition, Development and Maintenance

A.14 System acquisition, development and maintenance

A.14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

A.14.2.1 Secure development policy

Control

Rules for the development of software and systems shall be established and applied to developments within the organization.

A.14.2.2 System change control procedures

Control

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

A.14 – System Acquisition, Development and Maintenance

A.14.2.3 Technical review of applications after operating platform changes

Control

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

A.14.2.4 Restrictions on changes to software packages

Control

Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

A.14 – System Acquisition, Development and Maintenance

A.14.2.5 Secure system engineering principles

Control

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

A.14.2.6 Secure development environment

Control

Organizations shall establish and appropriately protect secure development environments for system development and integra-tion efforts that cover the entire system development lifecycle.

A.14 – System Acquisition, Development and Maintenance

A.14.2.7 Outsourced development

Control

The organization shall supervise and monitor the activity of out-sourced system development.

A.14.2.8 System security testing

Control

Testing of security functionality shall be carried out during development.

A.14.2.9 System acceptance testing

Control

Acceptance testing programs and related criteria shall be estab- lished for new information systems, upgrades and new versions.

A.14 – System Acquisition, Development and Maintenance

A.14 System acquisition, development and maintenance

A.14.3 Test data

Objective: To ensure the protection of data used for testing.

A.14.3.1 Protection of test data

Control

Test data shall be selected carefully, protected and controlled.

A.15 – Supplier Relationships

A.15 Supplier relationships

A.15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

A. 15.1.1 Information security policy for supplier relationships

Control

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A. 15.1.2 Addressing security within supplier agreements

Control

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

A.15 – Supplier Relationships

A.15 Supplier relationships

A.15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

A. 15.1.3 Information and communication technology supply chain

Control

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

A.15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with sup- plier agreements.

A. 15.2.1 Monitoring and review of supplier services

Control

Organizations shall regularly monitor, review and audit supplier service delivery.

A.15 – Supplier Relationships

A.15 Supplier relationships

A.15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with sup- plier agreements.

A. 15.2.2 Managing changes to supplier services

Control

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

A.16 – Information Security Incident Management

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A. 16.1.1 Responsibilities and procedures

Control

Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A. 16.1.2 Reporting information security events

Control

Information security events shall be reported through appropriate management channels as quickly as possible.

A.16 – Information Security Incident Management

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A. 16.1.3 Reporting information security weaknesses

Control

Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in sys-terns or services.

A. 16.1.4 Assessment of and decision on information security events

Control

Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

A.16 – Information Security Incident Management

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A. 16.1.5 Response to information security incidents

Control

Information security incidents shall be responded to in accordance with the documented procedures.

A. 16.1.6 Learning from information security incidents

Control

Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

A. 16.1.7 Collection of evidence

Control

The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

A.17 – Information Security Aspects of Business Continuity Management

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity

Objective: Information security continuity shall be embedded in the organization's business continuity management systems.

A. 17.1.1 Planning information security continuity

Control

The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

A. 17.1.2 Implementing information security continuity

Control

The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

A.17 – Information Security Aspects of Business Continuity Management

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity

Objective: Information security continuity shall be embedded in the organization's business continuity management systems.

A. 17.1.3 Verify, review and evaluate information security continuity

Control

The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

A.17.2 Redundancies

Objective: To ensure availability of information processing facilities.

A. 17.2.1 Availability of information processing facilities

Control

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

A.18 – Compliance

A.18 Compliance

A.18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A. 18.1.1 Identification of applicable legislation and contractual requirements

Control

All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

A. 18.1.2 Intellectual property rights

Control

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary soft- ware products.

A.18 – Compliance

A.18 Compliance

A.18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A. 18.1.3 Protection of records

Control

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

A. 18.1.4 Privacy and protection of personally identifiable information

Control

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

THANKS!