EU Twinning Project on
Statistics in Jordan

1949
دائرة الإحصاءات العامة
Department of Statistics

# Introduction of ISO/IEC 27001 Standard

## Activity 1.4.6:
## Security policy and data confidentiality

Amman, 8th January 2024

# Agenda

- Why ISO/IEC 27001
- ISO/IEC 27001 basic concepts
- ISO/IEC 27001 requirements
- ISO/IEC 27001 controls

# International standards organisations

- ISO (International Organization for Standardization) and IEC (the International Electrotechnical Commission) are independent, non-governmental international organization with a membership of many national standards bodies, that participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.
- The third edition of the standard (ISO/IEC 27001:2022) was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*

# Information security

- All information held and processed by an organization is subject to threats of attack, error, nature (for example, flood or fire), etc., and is subject to vulnerabilities inherent in its use. The term information security is generally based on information being considered as an asset which has a value requiring appropriate protection, for example, against the loss of availability, confidentiality and integrity.
- Information security involves the application and management of appropriate controls that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing consequences of information security incidents.

# Why ISO/IEC 27001

- Information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the information security that can be achieved through technical means is limited, and can be ineffective without being supported by appropriate management and procedures.

# Why ISO/IEC 27001

- ISO/IEC 27001 accreditation promotes a security-conscious organizational culture and ensures continued compliance and improvement
- ISO/IEC 27001 is not a legal requirement, none of the controls are universally mandatory for compliance, but adoption of the international security standard ensures best security practices and strategies to strengthen information security in an organisation.
- The implementation of ISO/IEC 27001 may reduce the chance of suffering a data breach and losing users trust as a result.

# ISO/IEC 27001: basic concepts

- Information Security Management System: an ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, to protect its information assets.
- It is based on a risk assessment and the organisation's risk acceptance levels, and is designed to effectively address and manage risks.
- The adoption of an ISMS is expected to be a strategic decision for an organization and it is necessary that this decision is seamlessly integrated, scaled and updated in accordance with the needs of the organization.

# Fundamental principles of an ISMS

- Awareness of the need for information security
- Assignment of responsibility for information security
- Management commitment
- Incorporating stakeholder interests
- Risk assessment to determine appropriate controls to achieve an acceptable level of risk
- Integrating security as an essential element of projects and information systems
- Active prevention and detection of information security incidents
- Continual reassessment of information security and making changes where necessary

# ISO/IEC 27001 requirements

The standard is broken down into Clauses which every organisation that intends to be ISO/IEC 27001 compliant is required to follow.

- **Context of the organisation**
- **Leadership**
- **Planning**
- **Support**
- **Operation**
- **Performance Evaluation**
- **Improvement**

# ISO/IEC 27001 requirements

## Context of the organisation

- The purpose of this clause is to ensure that the organisation establishes, implements, maintains and continually improves an information security management system, has a comprehensive understanding of its internal and external environment, identifies and understands the needs and expectations of its stakeholders, defines the boundaries and scope of the organisation's information security management system in order to effectively manage its information security risks.

# ISO/IEC 27001 requirements

## Leadership

- This requirement explains that the organisation’s top management must demonstrate leadership and commitment to the information security management system. Management shall monitor and evaluate the ISMS to ensure its effectiveness.
- The organization must have an information security policy that is approved by top management. This policy serves as a guideline for managing the organisation’s information security and should consider various factors such as business strategy, regulations, legislation, and information security risks and threats.
- Roles, responsibilities and authorities relating to information security must be defined and assigned by the organisation.

# ISO/IEC 27001 requirements

## Planning

- The organisation is required to define and apply an information security risk assessment process to identify, analyze and evaluate the information security risks.
- Based on the risk acceptance criteria, an information security risk treatment process shall be defined and applied to select appropriate information security risk treatment options and determine all controls necessary to implement the information security risk treatment. A list of necessary controls is provided by the standard (Annex A)
- The organisation must establish information security objectives and develop a plan to achieve them. Regular review of information security objectives and plans is necessary to ensure their relevance and effectiveness. Any changes in the organisation should be considered and incorporated into the plans.

# ISO/IEC 27001 requirements

## Support

- This clause ensures that the organisation has the necessary resources to maintain the security of its information systems. This includes identifying and documenting the personnel, hardware, software and other resources required for information security. The organisation shall ensure that these resources are available and accessible when required and that the personnel are competent and aware of the importance of information security and their roles and responsibilities in maintaining it.
- The organization must establish effective communication practices with relevant stakeholders to ensure information security objectives are met.
- Everything related to the ISMS must be documented and updated.

# ISO/IEC 27001 requirements

## Operation

- This requirement is focused on ensuring the security of an organisation’s information by planning and controlling its operations. This involves identifying and assessing risks associated with the organisation’s operations and implementing appropriate security controls to mitigate those risks.

# ISO/IEC 27001 requirements

## Performance evaluation

- This clause requires the organisation to evaluate how the ISMS is performing and look at the effectiveness of the information security management system.  The organisation shall determine what needs to be monitored and measured, including information security processes and controls, and the methods for monitoring, measurement, analysis and evaluation.
- The organisation shall conduct regular internal audits at planned intervals to assess the information security management system and provide information on whether the information security management system is effectively implemented and maintained and meets the organisation's requirements.
- The organization is also required to conduct regular management reviews to evaluate how the ISMS is performing and look at the effectiveness of the ISMS.

# ISO/IEC 27001 requirements

## Improvement

- The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system. This means that the organisation need to regularly review and update their ISMS to ensure its alignment with the organisation’s objectives, legal and regulatory requirements, and the ISO/IEC 27001 standard.
- The continual improvement process should be monitored and reviewed to ensure its effectiveness, and any necessary changes should be made to enhance the suitability, adequacy, and effectiveness of the ISMS.

# Risk assessment

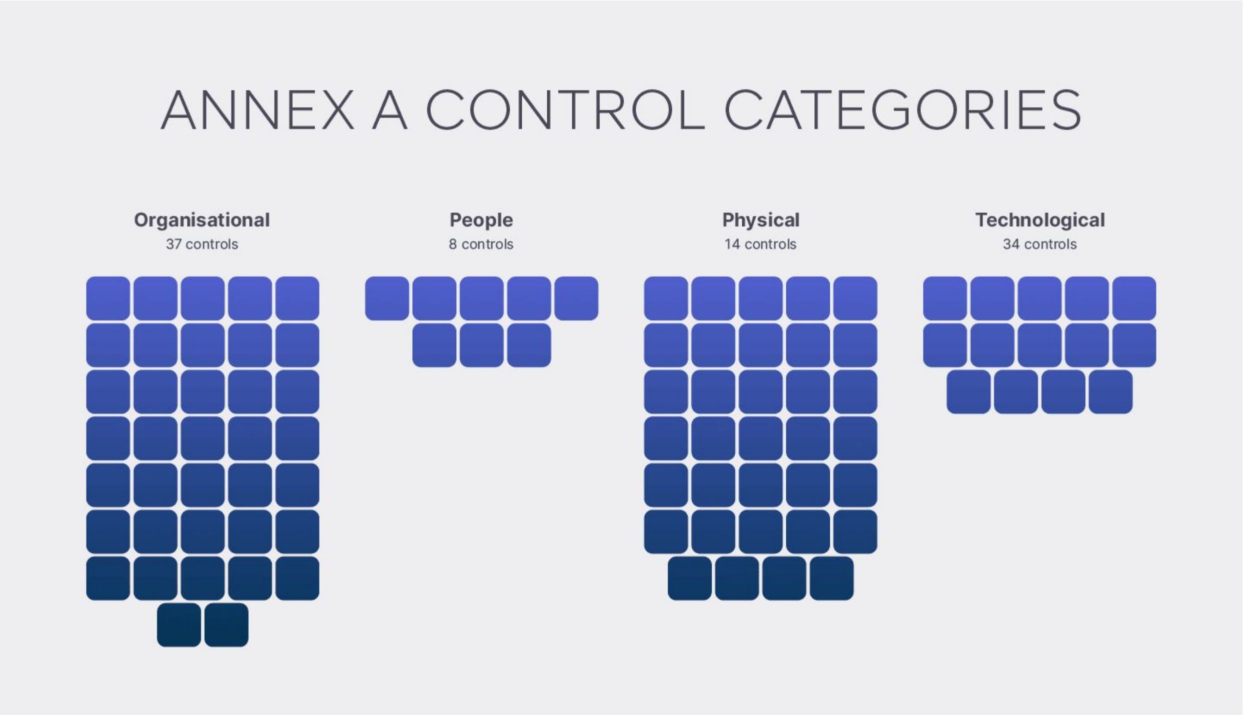
- Risk assessment should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.
- Risk assessment include:
  - the systematic approach of estimating the magnitude of risks (risk analysis)
  - the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).
- Risk assessment should be performed periodically to address changes in the information security requirements and in the risk situation.

# Risk treatment

- The organization should define criteria for determining whether or not risks can be accepted, for example, if it is assessed that the risk is low or that the cost of treatment is not cost-effective for the organization.
- For each of the risks identified following the risk assessment, a risk treatment decision needs to be made. Possible options are:
  - applying appropriate controls to reduce the risks;
  - accepting risks, providing they satisfy the organization’s policy and criteria for risk acceptance;
  - avoiding risks by not allowing actions that would cause the risks to occur;
  - sharing the associated risks to other parties, for example insurers or suppliers.
- For those risks where the risk treatment decision has been to apply appropriate controls, these controls should be selected and implemented.

# ISO/IEC 27001 Annex A

- Annex A in ISO/IEC 27001 is a part of the standard that lists a set of classified security controls that organisations use to demonstrate compliance with ISO/IEC 27001



# ISO/IEC 27001 Annex A

- **Organisational controls:** are the rules and measures that govern an organisation's overall approach to data protection across a wide range of issues. These controls include policies, rules, processes, procedures, organisational structures and more..
- **People controls:** regulate the human component of their information security programme by defining how employees interact with data and equipment. These controls cover secure personnel management, personnel security, and awareness and training.

# ISO/IEC 27001 Annex A

- **Physical controls:** are measures used to ensure the security of physical assets. These can include entry systems, guest access protocols, asset disposal procedures, storage media protocols and clear desk policies and are essential for the protection of confidential information.
- **Technological controls:** are digital rules and procedures that organisations should adopt to implement a protected, compliant IT infrastructure, from authentication techniques to and information logging.

# Working towards ISO/IEC 27001 compliance

The following best practices checklist can prepare ISO 27001 certification.

- Consult with the stakeholders and identify their information security expectations
- Define the scope of the ISMS and information security controls
- Lay out a clear security policy
- Identify information assets and their associated information security requirements
- Conduct a risk assessment to identify any existing and potential information security risks
- Assess information security risks and treat information security risks
- Select and implement relevant controls to manage unacceptable risks
- Continuously evaluate the strength of information security practices and assess risks on a regular basis
- Monitor, maintain and improve the effectiveness of controls associated with the organization’s information assets

EU Twinning Project on
Statistics in Jordan

DOS
1949
دائرة الإحصاءات العامة
Department of Statistics

# Thank you for your attention and support