ISO27001:2022
Lec3

7 – Support (Resources & Competence)

7.1 Resources

- The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

7 .2 Competence

- The organization shall:
  a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;
  b) ensure that these persons are competent on the basis of appropriate education, training, or experience;
  c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
  d) retain appropriate documented information as evidence of competence.

7 – Support (Awareness & Communication)

7.3 Awareness

- Persons doing work under the organization's control shall be aware of:

  a) the information security policy;
  b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
  c) the implications of not conforming with the information security management system requirements.

7.4 Communication

- The organization shall determine the need for internal and external communications relevant to the information security management system including:

  a) on what to communicate;
  b) when to communicate;
  c) with whom to communicate;
  d) who shall communicate; and
  e) the processes by which communication shall be effected.

7 – Support (General & Creating and updating)

7.5.1 General

- The organization's information security management system shall include:
  a) documented information required by this International Standard; and
  b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE: The extent of documented information for an information security management system can differ from one organization to another due to:

1. the size of organization and its type of activities, processes, products and services;
2. the complexity of processes and their interactions; and
3. the competence of persons.

7.5.2 Creating and updating

- When creating and updating documented information the organization shall ensure appropriate:

  a) identification and description (e.g., a title, date, author, or reference number);
  b) format (e.g., language, software version, graphics) and media (e.g., paper, electronic); and
  c) review and approval for suitability and adequacy.

7 – Support (Documented Information)

7.5 Documented information

7.5.3 Control of documented information

- Documented information required by the information security management system and by this International Standard shall be controlled to ensure:
  a) it is available and suitable for use, where and when it is needed; and
  b) it is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and
f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE: Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 – Operation (Planning & Control)

8.1 Operation planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

8 – Information Security Risk During the Operation

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2. a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

9 – Performance & Evaluation (Monitoring & Evaluation)

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE The methods selected should produce comparable and reproducible results to be considered valid.

c) when the monitoring and measuring shall be performed;
d) who shall monitor and measure;
e) when the results from monitoring and measurement shall be analysed and evaluated; and
f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9 – Performance & Evaluation (Internal Audit)

9.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to:
   1) the organization's own requirements for its information security management system; and
   2) the requirements of this International Standard;

b) is effectively implemented and maintained.

The organization shall:

c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
d) define the audit criteria and scope for each audit;
e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
f) ensure that the results of the audits are reported to relevant management; and
g) retain documented information as evidence of the audit programme(s) and the audit results.

9 – Performance & Evaluation (Management review)

9.3 Management review

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the information security management system;
c) feedback on the information security performance, including trends in:
    1) nonconformities and corrective actions;
    2) monitoring and measurement results;
    3) audit results; and
    4) fulfilment of information security objectives;
d) feedback from interested parties;
e) results of risk assessment and status of risk treatment plan; and
f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.
The organization shall retain documented information as evidence of the results of management reviews.

10.1 – Improvement (Nonconformity & Corrective Actions)

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:
   1) take action to control and correct it; and
   2) deal with the consequences;
b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   1) reviewing the nonconformity;
   2) determining the causes of the nonconformity; and
   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;
d) review the effectiveness of any corrective action taken; and
e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:

f) the nature of the nonconformities and any subsequent actions taken, and
g) the results of any corrective action.

10.2 – Improvement (Continual Improvement)

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

ISO27K – Clauses (4 - 10)

ISO 27001 Management system clauses

1, 2 & 3 Scope, normative references and terms and definitions.

4 Internal and external issues that may be relevant to the business and to the achievement of the objectives of the ISMS. Includes confirming interested parties and scope.

5 How top management will support the ISMS by creating roles and measures to implement and monitor it. Includes developing an information security policy aligned to business objectives.

6 How the organisation creates actions to address risks. Includes setting information security objectives.

7 Securing the right resources, the right people and the right infrastructure to manage and maintain the ISMS.

8 How the plans and processes will be executed, including documentation that needs to be produced.

9 How the organisation will monitor, measure, analyse and evaluate the ISMS.

10 Corrective action and continual improvement requirements.

THANKS!