***University of Oslo***
***Cybersecurity Governance***

# Summary of ISO/IEC 27001 ISMS Requirements

Instructional resource for studying.

## *Background:* JTC 1, SC 27, WG 1

In 1987, ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) established a cooperative body called JTC 1 (Joint Technical Committee No.1) with the purpose of standardizing information technology.
Wikipedia: https://en.wikipedia.org/wiki/ISO/IEC_JTC_1

There are approximately 40 subcommittees (SC) under JTC 1 that work with standardization in various IT areas. SC 27 focuses on information security.
Wikipedia: https://en.wikipedia.org/wiki/ISO/IEC_JTC_1/SC_27

There are 5 working groups (WG) under SC 27 that work on standardization of information security in various IT security areas. WG 1 focuses on the management of information security.
Wikipedia: https://en.wikipedia.org/wiki/Information_security_management

Standards maintained by WG 1 include:
ISO/IEC 27000: Overview
ISO/IEC 27001: Information Security Management System (ISMS) - Requirements
ISO/IEC 27002: Information Security Controls

ISO/IEC 27001 is a so-called "management system standard". Examples of other management system standards are:

- ISO 9001 Quality Management
- ISO/IEC 20000 Service Management
- ISO 22000 Food Safety Management System
- ISO 22300 Security and Resilience
- ISO/IEC 27001(ISMS: Information Security Management System)
- ISO 31000 Risk management
- ISO 39001 Road Safety Management System
- ISO/IEC 42001 AI Management System

The different standards for management systems have a common structure.
The common structure is defined by Annex SL: https://committee.iso.org/home/jtcg
This makes the management system standards more applicable and is particularly useful for organizations that need multiple management systems.

## *The structure of ISO/IEC 27001*

The table below lists the clauses and structure of ISO/IEC 27001:2022.

| | | | | |
|---|---|---|---|---|
| 1. Scope | | | | |
| 2. Normative references | | | | |
| 3. Terms and definitions | | | | |
| 4. Context of the organization | | | | |
| 4.1. Understanding the organisation and its context | 4.2. Understanding the needs and expectations of interested parties | 4.3. Determining the scope of the ISMS | 4.4. ISMS | |
| 5. Leadership | | | | |
| 5.1. Leadership and commitment | 5.2 Policy | 5.3. Organizational roles, responsibilities and authorities | | |
| 6. Planning | | | | |
| 6.1. Actions to address risks and opportunities | 6.2. Information security objectives and planing to achieve them | | | |
| 7. Support | | | | |
| 7.1. Resources | 7.2. Competence | 7.3. Awareness | 7.4. Communication | 7.5. Documentation |
| 8. Operation | | | | |
| 8.1. Operational planning and control | 8.2. Information security risk assessment | 8.3. Information security risk treatment | | |
| 9. Performance evaluation | | | | |
| 9.1. Monitoring, measurement, analysis and evaluation | 9.2. Internal audit | 9.3. Management review | | |
| 10. Improvement | | | | |
| 10.1. Continuous improvement | 10.2. Identify deviations and implement measures | | | |

Clauses 4-10 of ISO/IEC 27001 describe the requirements which are briefly summarised below.

**Clause 4: Context of the organization**

A holistic requirement is that the organization should establish, implement, maintain, and continuously improve an ISMS, which includes the necessary processes and their interactions, in accordance with all the requirements of the standard.

The organization shall identify external and internal aspects, conditions relevant to its purpose and that affect information security. For example, regulatory compliance requirements and industry norms are important external conditions. Furthermore, the organization must understand the information security needs and expectations of relevant 3rd parties that the company comes into contact with and must relate to.

The scope of the organization's ISMS shall be determined based on needs and the size of the organization.

**Clause 5: Leadership**

Senior management shall demonstrate leadership by, among other things, ensuring that information security policies and objectives are established and compatible with the organization's overall strategy, ensuring adequate resources for information security work, and communicating the importance of information security to the entire organization, and checking that the ISMS achieves the expected results.

Senior management must ensure that responsibility and authority for roles relevant to information security are assigned and communicated internally in the organisation.

**Clause 6: Planning**

The organization must plan for risk management by choosing a method for risk assessment, defining criteria for risk acceptance. Furthermore, the organization must establish a process to address identified risks.

When selecting security controls to reduce risk to an acceptable level, or to satisfy regulatory requirements, the organization shall take into account the list of security controls in Annex A (and as described in detail in ISO/IEC 27002). In addition, other security controls may be considered.

The SoA (Statement of Applicability) is a document that lists all the security controls in Annex A, and which for each control briefly explains whether, and why, the control has been implemented or not. When a risk assessment is carried out (as part of Clause 8: Operation below) and ways of managing the risks are chosen, a SoA shall be prepared which shall contain at least:

- necessary information security controls
- justification for their inclusion;
- whether or not the necessary security controls have been implemented; and
- the grounds for excluding some of the controls in Annex A.

The organization will establish information security objectives for relevant domains, functions, and business processes, which means specifying confidentiality, integrity, and availability (KIT) needs. If practically possible, it must be measured and documented whether the objectives are achieved.

**Clause 7: Support**

The organisation shall allocate sufficient resources needed for the work on the ISMS. The organisation must identify the need for the competence and ensure that relevant employees actually have that competence.

The organization must ensure that employees have awareness of security policies, the importance of following policies, and the consequences of not following policies. The organisation shall have a plan for communication regarding information security, both internally and with various external parties.

Documentation is a basic requirement. The organisation's ISMS shall include documented information that is explicitly required by the standard, and documented

information that is necessary for the effectiveness of the entire ISMS, including about the various processes involved. The scope of documentation can vary depending on the size of the organization and its type of activities, processes, products and services, the complexity of processes and their interactions, and the competencies of people.

**Clause 8: Operation.**

The organization shall plan, implement and manage the processes and security controls necessary to meet the requirements of the ISMS, and to operate the activities related to the management of risk and management of security measures described under point Clause 6: Planning.

The organisation must designate relevant domains, functions and business processes for assessing information security risks. The assessment shall consist of mapping assets, identifying threats and vulnerabilities, estimating likelihood and consequence of risks, which ultimately forms the basis for computing risk levels.

Based on the risk assessment and criteria for risk acceptance, as well as regulatory compliance requirements, the organization must determine and implement treatment of the various risks, which may be reducing risk by implementing security controls, transferring risk e.g. by purchasing cyber insurance, accepting risk based on the level of acceptable risk, or avoiding risk by stopping the business process that entails risk.

The organisation must keep documented information about risk assessments and how the risks have been treated.

**Clause 9: Performance evaluation**

For monitoring, measuring, analysing and evaluating the ISMS, the organisation must decide what needs to be monitored and measured, as well as methods for this. The methods chosen should provide comparable and reproducible results to be considered valid.

The organisation shall carry out internal audits at scheduled intervals to provide information on whether the ISMS is functioning as planned.
Senior management shall review the organisation's ISMS at scheduled intervals to ensure continuous suitability, adequacy and efficiency.

The management review shall include, among other things, an assessment of the status of action items from previous management reviews, changes in external and internal conditions relevant to information security, threat and risk assessments, and how risk has been treated.

The results of the management review shall include decisions related to continuous improvement opportunities and any need for changes in the ISMS. The management review must be documented.

**Clause 10: Improvement.**

The organisation shall continuously improve the suitability, adequacy and effectiveness of the ISMS.

When weaknesses or nonconformities in the ISMS are identified, the organization shall take action to correct it, address possible consequences, and assess the need for action to eliminate the causes of nonconformities so that they do not recur or occur elsewhere.