Introduction to ISO 27001:2013

Document number	20200606
Author	P.Leclercq - pl@osix.be
Owner	P.Leclercq
Version	1.1
Date	2020-06-06
Status	Released
Security level	Public

Table of Contents

Introduction

Definition

ISO 27001 is an international standard published by the International Standardization Organization (ISO); it describes the requirements to establish, implement, maintain and improve an information security management system in a company. The latest revision of this standard was published in 2013, and its full title is now ISO/IEC 27001:2013. The first revision of the standard was published in 2005, and was developed based on the British standard BS 7799-2.

Goal

The goal of ISO 27001 is to protect information confidentiality, integrity and availability (CIA triad) based on a risk management process.

The standard is normative and not prescriptive : it does not tell how to implement the requirements, but no requirement from sections 4 to 10 may be ignored to get certified.

Structure

The ISO 27001:2013 standard is a 23 pages document, divided in 11 sections and one Annex:

- Clause 0 : introduction
- Clause 1 : scope
- Clause 2 : normative reference
- Clause 3 : terms and definitions
- Clause 4 : context of the organization
- Clause 5 : leadership
- Clause 6 : planning
- Clause 7 : support
- Clause 8 : operation
- Clause 9: performance evaluation
- Clause 10: improvement
- Annex A: reference control objectives and controls. The controls can be technical, organisational, or human resource related.

The Annex A itself contains 14 sections with 114 controls.

Each clause (from 4 to 10) lists the documents, mandatory or not, that must or should be produced. There are 16 mandatory documents (highlighted in yellow in this document) and 6 mandatory records (highlighted in blue).

The standard has a structure compatible with standards for other management systems (e.g. ISO 9001, ISO 22301...)

Implementation Project

The standard suggests that the implementation of ISO 27001 happens in the scope of a project (or set of projects), and that the whole lifecycle of the ISMS follows the Deming Plan Do Check Act (PDCA) cycle:

- Plan: clauses 4 to 7;
- Do: clause 8;
- Check: clause 9;
- Act: clause 10.

Clause 4: Context of the Organisation

Clause 4.1: Understanding the Organisation and its Context

This clause requires that the organisation determines internal and external issues influencing the security of its information.

The assessment should be based on ISO 31000:2009.

The documentation of this assessment is not mandatory.

External issues can be:

- Social and cultural environment;
- Legal and regulatory environment;
- Financial environment;
- Technological environment;
- Economic environment;
- Natural environment;
- Political environment;
- Competitive environment.

Internal issues can be:

- Governance and organisational structure;
- Policies, standards, guidelines and strategy;
- Available resources and knowledge;
- IT infrastructure;
- Internal stakeholders;
- Contractual relationships.

Clause 4.2: Understanding the Needs and Expectations of Interested Parties

This clause requires that the organisation identifies the interested parties, and identifies their requirements.

Interested parties can be:

- Employees;
- Clients;
- Partners;
- Suppliers;
- Local authorities.

The documentation of this assessment is not mandatory.

Clause 4.3: Determining the Scope of the ISMS

The organisation shall determine the boundaries and applicability of the ISMS to establish its scope.

The determination of the scope must consider the issues identified in 4.1, the requirements identified in 4.2, and the interfaces and dependencies between actions performed by the organisation and other organisations.

Then, the organisation shall define the activities, services, products and locations to which the ISMS will apply. It is not mandatory to cover all the organisation; only a subset of the company can be subject to the standard and certified.

The scope document is mandatory and should list the activities, services, products and locations to which the ISMS will apply.

Clause 4.4: Information Security Management System

This clause requires the organisation to establish, maintain and improve an ISMS according to this standard.

Clause 5: Leadership

Clause 5.1: Leadership and Commitment

ISO 27001 requires that the top management demonstrates leadership and commitment towards the respect of the ISMS.

The standard expects the following actions from the management:

- Establish an information security policy and objectives in line with the strategy of the organisation;
- Ensure the ISMS is integrated into the organisation processes;
- Provide resources for the implementation, execution and improvement of the ISMS;
- Promote the adherence to the ISMS and its continual improvement;
- Measure the ISMS outcomes.

The recording of these intentions is not mandatory, but it is a good idea to document the management responsibilities.

Clause 5.2: Security Policy

The top management is required to establish, document and communicate an information security policy.

This policy will document:

- Security Objectives (or a framework to establish security objectives);
- A commitment to satisfy the requirements related to information security;
- A commitment to continually improve the ISMS.

Clause 5.3: Organisational roles, Responsibilities and Authorities

Top management shall assign responsibility and authority for:

- Ensuring the ISMS conforms to this standard;
- Reporting on the performance of the ISMS to management or within the organisation.

Clause 6: Planning

Clause 6.1: Actions to Address Risks and Opportunities

6.1.1: General

When planning the ISMS, the organisation will consider the requirements gathered in 4.1 and 4.2.

It will determine the risks and opportunities to be addressed so the ISMS achieves its goals and can be improved.

It will then plan the actions to address these risks and opportunities.

6.1.2: Risk Assessment

The organisation shall define and apply a risk assessment process.

The process must define criteria for:

- Performing a risk assessment;
- Accepting the risk.

The process must ensure repeated risk assessments produce comparable results.

The process must identify loss of confidentiality, integrity and availability (CIA) for information.

Each risk must be assigned to an owner.

According to ISO 31000:2009, the risk assessment process must contain the following phases:

- Risk identification: list the CIA risks and assign risk owners;
- Risk analysis: determine consequences, likelihood and overall risk level;
- Risk evaluation: compare risk level with the criteria defined above and prioritise the risks for treatment.

The process must be documented.

Executing the risk assessment is the first part of the planning phase.

6.1.3: Risk Treatment

The organisation must define, apply and document a risk treatment process.

The process must contain the following steps:

- Select risk treatment options (mitigate, accept, transfer, avoid);
- Determine all controls needed to implement the treatment;
- Check the controls with the Annex A and ensure none have been omitted;
- Write a Statement of Applicability, containing the list of controls to be applied, whether they are implemented or not, and a justification for inclusion or exclusion;
- Write a risk treatment plan;
- Obtain risk owners' approval for the risk treatment and acceptance of the residual risks.

The risk treatment process, Statement of Applicability and treatment plan must be documented.

Clause 6.2: Information Security Objectives and Planning

The organisation must establish security objectives:

- That are in line with the security policy;
- That are measurable;
- In line with the requirements, risk assessment and risk treatment.

Security objectives must be documented, communicated and updated.

The planning to realise the objectives must contain:

- What will be done;
- Needed resources;
- Who will be responsible;
- Schedule;
- How the results will be evaluated.

Clause 7: Support

Clause 7.1: Resources

The organisation must determine and provide the resources to create, implement, maintain and improve the ISMS.

Implementation resources are documented in clause 6.2.

Clause 7.2: Competence

The organisation must determine the necessary competences of the resources concerned by the ISMS.

Then, it must ensure the used resources have these competences based on education, training or experience.

If needed, it takes action to acquire these competences by training, mentoring, hiring of external staff.

The evidence of competences, training and skills must be recorded.

Clause 7.3: Awareness

All persons working for the organisation must be informed and aware of the security policy, how they contribute to the security, and the implications of not conforming with the security requirements.

Clause 7.4: Communication

The organisation must elaborate a communication plan regarding the ISMS, including the answers to the following questions: what, when, with whom, who, how.

Clause 7.5: Documentation

The ISMS must include documentation as required by this standard, and deemed necessary for the its effectiveness.

The extent of the documentation is influenced by the size of the organisation, the complexity of its processes, and the competences of its resources.

The organisation must ensure the documentation carries appropriate attributes:

- Identification (title, date, author, reference, …);
- Format (language, graphics, software used, ...) and media (paper, electronic, …);
- Review and approval.

The following properties of the documentation must be controlled:

- Availability: distribution, access, retrieval;
- Protection: storage, preservation, control of changes, retention and disposition.

External documentation needed by the ISMS must be identified and controlled.

Clause 8: Operation

This clause concerns the 'Do' phase of the cycle.

Clause 8.1: Operational Planning and Control

The organisation shall plan, implement and control the processes described in the planning phase to assess the risks and treat them to achieve the selected security objectives (6.1 and 6.2).

The documentation showing that the processes have been carried out must be kept.

Clause 8.2: Information Security Risk Assessment

The organisation shall perform risk assessments at planned intervals or when significant changes occur.

The risk assessments must be documented.

Clause 8.3: Information Security Risk Treatment

The organisation shall implement the risk treatment plan.

The results of the risk treatment must be documented.

Clause 9: Performance Evaluation

This clause concerns the 'Check' phase of the cycle.

Clause 9.1: Monitoring, Measurement, Analysis and Evaluation

The organisation must evaluate the security performance and the ISMS effectiveness.

The following items of the check process must be defined and documented:

- Which processes and controls must be monitored and measured;
- How to monitor, measure, analyse and evaluate;
- When the monitoring and measurements will be performed;
- Who shall monitor and measure;
- When the results will be analysed and evaluated;
- Who shall analyse and evaluate the results.

The results of the monitoring and measurements must be recorded.

Clause 9.2: Internal Audit

The organisation shall conduct internal audits at planned intervals.

The audits must ensure the ISMS conforms to its own requirements and this standard's requirements and is effectively implemented and maintained.

The organisation must plan, establish, maintain and document an internal audit programme containing:

- When: Planning, with frequencies;
- How: methods;
- Who: responsibilities.

Each audit must:

- Take into account the results of the previous audits;
- Define the audit criteria and scope;
- Select auditors to ensure objectivity and impartiality;
- Ensure results are reported to management;
- Retain documentation of audit results.

Clause 9.3: Management Review

Top management must review the ISMS at planned intervals to ensure its suitability, adequacy and effectiveness.

The reviews must contain:

- Status of actions of previous reviews;
- Considerations of changes in external and internal issues;
- Feedback on ISMS performance (nonconformities, corrective actions, results of monitoring and measurements, audit results, fulfilment of security objectives);
- Feedback from interested parties;
- Results of risk assessments and status of risk treatment;
- Opportunities for continual improvement.

The outputs of the review must contain decisions related to continual improvement and needs for changes of the ISMS.

The results of the management reviews must be documented.

Clause 10: Improvement

This clause corresponds to the 'Act' phase of the PDCA cycle.

Clause 10.1: Nonconformity and Corrective Action

When a nonconformity occurs, the organisation must take action to correct it and deal with the consequences.

The following actions must be taken:

- Evaluate the nonconformity;
- Determine its root cause;
- Determine if similar nonconformity exist elsewhere;
- Implement needed actions;
- Review the effectiveness of corrective actions;
- Change the ISMS if needed.

The nonconformities, corrective actions and results must be documented.

Clause 10.2: Continual Improvement

The organisation must continually improve its ISMS.

Annex A: Reference Control Objectives

Control objectives are derived from the ISO 27002:2013 standard.

A.5: Information Security Policies

A.5.1: Management Direction

Objective: provide management direction for ISMS.

- Define a set of policies
- Maintain them

A.6: Organisation of Information Security

A.6.1: Internal Organisation

Objective: establish management framework

- Roles and responsibilities;
- Segregation of duties;
- Contact with authorities and special interest groups;

- Information security in project management.

A.6.2: Mobile Devices and Teleworking
Objective: ensure security of teleworking and mobile devices.

A7: Human Resource Security
A.7.1: Prior to Employment
Objective: ensure employees and contractors understand their future responsibilities and are fit for their future roles.

The responsibilities of employees and contractors must be documented.

A.7.2: During Employment
Objective: ensure employees and contractors understand their responsibilities and are fit for their roles.

A.7.3: Termination and Change of Employment
Objective: protect the organisation as part of the employment change.

A.8: Asset Management
A.8.1: Responsibility for Assets
Objective: identify organisational assets and define protection responsibilities.

The inventory of assets and acceptable use policy must be documented.

A.8.2: Information Classification
Objective: ensure information receives an appropriate level of protection.

A.8.3: Media Handling
Objective: prevent unauthorized disclosure or changes to the information.

The information must be classified (legal requirements, value, criticality, sensitivity) and labelled.

A.9: Access Control
A.9.1: Business Requirement of Access Control
Objective: limit access to information and IT processing facilities.

The access control policy must be documented.

A.9.2: User Access Management
Objective: ensure authorised and prevent unauthorised access to information.

A.9.3: User Responsibilities
Objective: make users accountable for their credentials.

A.9.4: System and Application Access Control
Objective: prevent unauthorised access to systems and applications.

A.10: Cryptography
A.10.1: Cryptographic Controls
Objective: ensure effective use of cryptography.

A.11: Physical and Environmental Security

A.11.1: Secure Areas

Objective: prevent unauthorised access to information processing facilities.

A.11.2: Equipment

Objective: prevent loss, damage or theft of assets.

A.12: Operations Security

A.12.1: Operational Procedures and Responsibilities

Objective: ensure correct and secure operations.

The operational procedures must be documented.

A.12.2: Protection from Malware

Objective: ensure protection against malware.

A.12.3: Backup

Objective: protect against loss of data.

A.12.4: Logging and Monitoring

Objective: record events and generate evidence.

The event logs, operator and administrator logs must be retained.

A.12.5: Control of Operational Software

Objective: ensure integrity of operational systems.

A.12.6: Technical Vulnerability Management

Objective: prevent exploitation of technical vulnerabilities.

A.12.7: Information Systems Audit Considerations

Objective: minimise the impact of audits on operational systems.

A.13: Communication Security

A.13.1: Network Security Management

Objective: ensure protection of information in the network.

A.13.2: Information Transfer

Objective: maintain security of information during transfers.

The non-disclosure agreements must be retained.

A.14: System Acquisition, Development and Maintenance

A.14.1: Security Requirements of Information Systems

Objective: ensure that information security is an integral part of the IT systems lifecycle.

A.14.2: Security in Development and Support Processes

Objective: ensure information security is designed and implemented in the development lifecycle.

The principles for engineering secure systems must be documented.

A.14.3: Test Data

Objective: ensure protection of test data.

A.15: Supplier Relationships

A.15.1: Information Security in Supplier Relationships

Objective: ensure protection of assets accessible by suppliers.

The supplier security policy must be documented.

A.15.2: Supplier Service Delivery Management

Objective: maintain an agreed level of security and service in supplier agreements.

A.16: Information Security Incident Management

A.16.1: Management of Information Security Incidents and Improvements

Objective: ensure consistent approach to security incidents.

The security incident management procedure must be documented.

A.17: Information Security Aspects of Business Continuity

A.17.1: Information Security Continuity

Objective: ensure information security continuity is part of the business continuity plan.

The business continuity plan must be documented.

A.17.2: Redundancies

Objective: ensure availability of IT processing facilities.

A.18: Compliance

A.18.1: Compliance with Legal and Contractual Requirements

Objective: avoid breach of obligations regarding information security.

The legislative, statutory, regulatory and contractual requirements must be documented.

A.18.2: Information Security Reviews

Objective: ensure information security complies with policies and procedures.

List of Mandatory Documents

Mandatory Documents

Scope of the ISMS	4.3
Information Security Policy and security objectives	5.2, 6.2
Risk assessment and risk treatment processes	6.1.2, 6.1.3
Statement of Applicability	6.1.3
Risk treatment plan	6.1.3, 6.2
Risk assessment and treatment results	8.2, 8.3
Definition of security roles and responsibilities	A.7.1
Inventory of assets	A.8.1
Acceptable use policy	A.8.1
Access control policy	A.9.1
Operating procedures for IT management	A.12.1
Principles for engineering secure systems	A.14.2
Supplier security policy	A.15.1
Information security incident management procedure	A.16.1
Business continuity procedures	A.17.1
Legal, statutory, regulatory and contractual requirements	A.18.1

Mandatory Records

Competences, trainings, skills and qualifications	7.2
Monitoring and measurement results	9.1
Audit programme	9.2
Audit results	9.2
Management reviews results	9.3
Nonconformities, corrective actions and results	10.1
Events, operators and administrator logs	A.12.4