INTERNATIONAL STANDARD

ISO/IEC 27003

Second edition
2017-03

Information technology — Security techniques — Information security management systems — Guidance

Technologies de l'information — Techniques de sécurité --Systèmes de management de la sécurité de l'information — Lignes directrices

Reference number
ISO/IEC 27003:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition of ISO/IEC 27003 cancels and replaces the first edition (ISO/IEC 27003:2010), of which it constitutes a minor revision.

The main changes compared to the previous edition are as follows:

— the scope and title have been changed to cover explanation of, and guidance on the requirements of, ISO/IEC 27001:2013 rather than the previous edition (ISO/IEC 27001:2005);

— the structure is now aligned to the structure of ISO/IEC 27001:2013 to make it easier for the user to use it together with ISO/IEC 27001:2013;

— the previous edition had a project approach with a sequence of activities. This edition instead provides guidance on the requirements regardless of the order in which they are implemented.

Introduction

This document provides guidance on the requirements for an information security management system (ISMS) as specified in ISO/IEC 27001 and provides recommendations ('should'), possibilities ('can') and permissions ('may') in relation to them. It is not the intention of this document to provide general guidance on all aspects of information security.

Clauses 4 to 10 of this document mirror the structure of ISO/IEC 27001:2013.

This document does not add any new requirements for an ISMS and its related terms and definitions. Organizations should refer to ISO/IEC 27001 and ISO/IEC 27000 for requirements and definitions. Organizations implementing an ISMS are under no obligation to observe the guidance in this document.

An ISMS emphasizes the importance of the following phases:

- understanding the organization's needs and the necessity for establishing information security policy and information security objectives;
- assessing the organization's risks related to information security;
- implementing and operating information security processes, controls and other measures to treat risks;
- monitoring and reviewing the performance and effectiveness of the ISMS; and
- practising continual improvement.

An ISMS, similar to any other type of management system, includes the following key components:

a) policy;

b) persons with defined responsibilities;

c) management processes related to:

   1) policy establishment;

   2) awareness and competence provision;

   3) planning;

   4) implementation;

   5) operation;

   6) performance assessment;

   7) management review; and

   8) improvement; and

d) documented information.

An ISMS has additional key components such as:

e) information security risk assessment; and

f) information security risk treatment, including determination and implementation of controls.

This document is generic and intended to be applicable to all organizations, regardless of type, size or nature. The organization should identify which part of this guidance applies to it in accordance with its specific organizational context (see ISO/IEC 27001:2013, Clause 4).

For example, some guidance can be more suited to large organizations, but for very small organizations (e.g. with fewer than 10 persons) some of the guidance can be unnecessary or inappropriate.

The descriptions of Clauses 4 to10 are structured as follows:

— **Required activity**: presents key activities required in the corresponding subclause of ISO/IEC 27001;

— **Explanation**: explains what the requirements of ISO/IEC 27001 imply;

— **Guidance**: provides more detailed or supportive information to implement "required activity" including examples for implementation; and

— **Other information**: provides further information that can be considered.

ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005 form a set of documents supporting and providing guidance on ISO/IEC 27001:2013. Among these documents, ISO/IEC 27003 is a basic and comprehensive document that provides guidance for all the requirements of ISO/IEC 27001, but it does not have detailed descriptions regarding "monitoring, measurement, analysis and evaluation" and information security risk management. ISO/IEC 27004 and ISO/IEC 27005 focus on specific contents and give more detailed guidance on "monitoring, measurement, analysis and evaluation" and information security risk management.

There are several explicit references to documented information in ISO/IEC 27001. Nevertheless, an organization can retain additional documented information that it determines as necessary for the effectiveness of its management system as part of its response to ISO/IEC 27001:2013, 7.5.1 b). In these cases, this document uses the phrase "Documented information on this activity and its outcome is mandatory only in the form and to the extent that the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b))."

Information technology — Security techniques — Information security management systems — Guidance

1 Scope

This document provides explanation and guidance on ISO/IEC 27001:2013.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2016 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

4 Context of the organization

4.1 Understanding the organization and its context

Required activity

The organization determines external and internal issues relevant to its purpose and affecting its ability to achieve the intended outcome(s) of the information security management system (ISMS).

Explanation

As an integral function of the ISMS, the organization continually analyses itself and the world surrounding it. This analysis is concerned with external and internal issues that in some way affect information security and how information security can be managed, and that are relevant to the organization's objectives.

Analysis of these issues has three purposes:

- understanding the context in order to decide the scope of the ISMS;
- analysing the context in order to determine risks and opportunities; and
- ensuring that the ISMS is adapted to changing external and internal issues.

External issues are those outside of the organization’s control. This is often referred to as the organization’s environment. Analysing this environment can include the following aspects:

a) social and cultural;

b) political, legal, normative and regulatory;

c) financial and macroeconomic;

d) technological;

e) natural; and

f) competitive.

These aspects of the organization’s environment continually present issues that affect information security and how information security can be managed. The relevant external issues depend on the organization’s specific priorities and situation.

For example, external issues for a specific organization can include:

g) the legal implications of using an outsourced IT service (legal aspect);

h) characteristics of the nature in terms of possibility of disasters such as fire, flood and earthquakes (natural aspect);

i) technical advances of hacking tools and use of cryptography (technological aspect); and

j) the general demand for the organization’s services (social, cultural or financial aspects).

Internal issues are subject to the organization’s control. Analysing the internal issues can include the following aspects:

k) the organization’s culture;

l) policies, objectives, and the strategies to achieve them;

m) governance, organizational structure, roles and responsibilities;

n) standards, guidelines and models adopted by the organization;

o) contractual relationships that can directly affect the organization’s processes included in the scope of the ISMS;

p) processes and procedures;

q) the capabilities, in terms of resources and knowledge (e.g. capital, time, persons, processes, systems and technologies);

r) physical infrastructure and environment;

s) information systems, information flows and decision making processes (both formal and informal); and

t) previous audits and previous risk assessment results.

The results of this activity are used in 4.3, 6.1 and 9.3.

Guidance

Based on an understanding of the organization’s purpose (e.g. referring to its mission statement or business plan) as well as the intended outcome(s) of the organization’s ISMS, the organization should:

— review the external environment to identify relevant external issues; and

— review the internal aspects to identify relevant internal issues.

In order to identify relevant issues, the following question can be asked: How does a certain category of issues (see a) to t) above) affect information security objectives? Three examples of internal issues serve as an illustration by:

Example 1 on governance and organizational structure (see item m)): When establishing an ISMS, already existing governance and organizational structures should be taken into account. As an example, the organization can model the structure of its ISMS based on the structure of other existing management systems, and can combine common functions, such as management review and auditing.

Example 2 on policy, objectives and strategies (see item l)): An analysis of existing policies, objectives and strategies, can indicate what the organization intends to achieve and how the information security objectives can be aligned with business objectives to ensure successful outcomes.

Example 3 on information systems and information flows (see item s)): When determining internal issues, the organization should identify, at a sufficient level of detail, the information flows between its various information systems.

As both the external and the internal issues will change over time, the issues and their influence on the scope, constraints and requirements of the ISMS should be reviewed regularly.

Documented information on this activity and its outcome is mandatory only in the form and to the extent that the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

In ISO/IEC 27000, the definition of “organization” has a note which states that: “The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.” Some of these examples are whole legal entities, whilst others are not.

There are four cases:

1) the organization is a legal or administrative entity (e.g. sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution whether incorporated or not, public or private);

2) the organization is a subset of a legal or administrative entity (e.g. part of a company, corporation, enterprise);

3) the organization is a set of a legal or administrative entities (e.g. a consortium of sole-traders, larger companies, corporations, firms); and

4) the organization is a set of subsets of legal or administrative entities (e.g. clubs, trade associations).

4.2 Understanding the needs and expectations of interested parties

Required activity

The organization determines interested parties relevant to the ISMS and their requirements relevant to information security.

Explanation

Interested party is a defined term (see ISO/IEC 27000:2016, 2.41) that refers to persons or organizations that can affect, be affected by, or perceive themselves to be affected by a decision or activity of the organization. Interested parties can be found both outside and inside the organization and can have specific needs, expectations and requirements for the organization’s information security.

External interested parties can include:

a) regulators and legislators;

b) shareholders including owners and investors;

c) suppliers including subcontractors, consultants, and outsourcing partners;

d) industry associations;

e) competitors;

f) customers and consumers; and

g) activist groups.

Internal interested parties can include:

h) decision makers including top management;

i) process owners, system owners, and information owners;

j) support functions such as IT or Human Resources;

k) employees and users; and

l) information security professionals.

The results of this activity are used in 4.3 and 6.1.

Guidance

The following steps should be taken:

— identify external interested parties;

— identify internal interested parties; and

— identify requirements of interested parties.

As the needs, expectations and requirement of interested parties change over time, these changes and their influence on the scope, constraints and requirements of the ISMS should be reviewed regularly.

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

No other information.

4.3 Determining the scope of the information security management system

Required activity

The organization determines the boundaries and applicability of the ISMS to establish its scope.

Explanation

The scope defines where and for what exactly the ISMS is applicable and where and for what it is not.

Establishing the scope is therefore a key activity that determines the necessary foundation for all other activities in the implementation of the ISMS. For instance, risk assessment and risk treatment, including the determination of controls, will not produce valid results without having a precise understanding of where exactly the ISMS is applicable. Precise knowledge of the boundaries and applicability of the ISMS and the interfaces and dependencies between the organization and other organizations is critical as well. Any later modifications of the scope can result in considerable additional effort and costs.

The following factors can affect the determination of the scope:

a) the external and internal issues described in 4.1;

b) the interested parties and their requirements that are determined according to ISO/IEC 27001:2013,4.2;

c) the readiness of the business activities to be included as part of ISMS coverage;

d) all support functions, i.e. functions that are necessary to support these business activities (e.g. human resource~~s~~ management; IT services and software applications; facility management of buildings, physical zones, essential services and utilities); and

e) all functions that are outsourced either to other parts within the organization or to independent suppliers.

The scope of an ISMS can be very different from one implementation to another. For instance, the scope can include:

- one or more specific processes;
- one or more specific functions;
- one or more specific services;
- one or more specific sections or locations;
- an entire legal entity; and
- an entire administrative entity and one or more of its suppliers.

Guidance

To establish the scope of an ISMS, a multi-step approach can be followed:

f) determine the preliminary scope: this activity should be conducted by a small, but representative group of management representatives;

g) determine the refined scope: the functional units within and outside the preliminary scope should be reviewed, possibly followed by inclusion or exclusion of some of these functional units to reduce the number of interfaces along the boundaries. When refining the preliminary scope, all support functions should be considered that are necessary to support the business activities included in the scope;

h) determine the final scope: the refined scope should be evaluated by all management within the refined scope. If necessary, it should be adjusted and then precisely described; and

i) approval of the scope: the documented information describing the scope should be formally approved by top management.

The organization should also consider activities with impact on the ISMS or activities that are outsourced, either to other parts within the organization or to independent suppliers. For such activities, interfaces (physical, technical and organizational) and their influence on the scope should be identified.

Documented information describing the scope should include:

j) the organizational scope, boundaries and interfaces;

k) the information and communication technology scope, boundaries and interfaces; and

l) the physical scope, boundaries and interfaces.

Other information

No other information.

4.4 Information security management system

Required activity

The organization establishes, implements, maintains and continually improves the ISMS.

Explanation

ISO/IEC 27001:2013, 4.4 states the central requirement for establishing, implementing, maintaining and continually improving an ISMS. While the other parts of ISO/IEC 27001 describe the required elements of an ISMS, 4.4 mandates the organization to ensure that all required elements are met in order to establish, implement, maintain and continually improve the ISMS.

Guidance

No specific guidance.

Other information

No other information.

5 Leadership

5.1 Leadership and commitment

Required activity

Top management demonstrates leadership and commitment with respect to the ISMS.

Explanation

Leadership and commitment are essential for an effective ISMS.

Top management is defined (see ISO/IEC 27000) as a person or group of people who directs and controls the organization of the ISMS at the highest level, i.e. top management has the overall responsibility for the ISMS. This means that top management directs the ISMS in a similar way to other areas in the organization, for example the way budgets are allocated and monitored. Top management can delegate authority in the organization and provide resources for actually performing activities related to information security and the ISMS, but it still retains overall responsibility.

As an example, the organization implementing and operating the ISMS can be a business unit within a larger organization. In this case, top management is the person or group of people that directs and controls that business unit.

Top management also participates in management review (see 9.3) and promotes continual improvement (see 10.2).

Guidance

Top management should provide leadership and show commitment through the following:

a) top management should ensure that the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) top management should ensure that ISMS requirements and controls are integrated into the organization's processes. How this is achieved should be tailored to the specific context of the organization. For example, an organization that has designated process owners can delegate the responsibility to implement applicable requirements to these persons or group of people. Top management support can also be needed to overcome organizational resistance to changes in processes and controls;

c) top management should ensure the availability of resources for an effective ISMS. The resources are needed for the establishment of the ISMS, its implementation, maintenance and improvement, as well as for implementing information security controls. Resources needed for the ISMS include:

   1) financial resources;

   2) personnel;

   3) facilities; and

   4) technical infrastructure.

   The needed resources depend on the organization's context, such as the size, the complexity, and internal and external requirements. The management review should provide information that indicates whether the resources are adequate for the organization;

d) top management should communicate the need for information security management in the organization and the need to conform to ISMS requirements. This can be done by giving practical examples that illustrate what the actual need is in the context of the organization and by communicating information security requirements;

e) top management should ensure that the ISMS achieves its intended outcome(s) by supporting the implementation of all information security management processes, and in particular through requesting and reviewing reports on the status and effectiveness of the ISMS (see 5.3 b)). Such reports can be derived from measurements (see 6.2 b) and 9.1 a)), management reviews and audit reports. Top management can also set performance objectives for key personnel involved with the ISMS;

f) top management should direct and support persons in the organization directly involved with information security and the ISMS. Failing to do this can have a negative impact on the effectiveness of the ISMS. Feedback from top management can include how planned activities are aligned to the strategic needs for the organization and also for prioritizing different activities in the ISMS;

g) top management should assess resource needs during management reviews and set objectives for continual improvement and for monitoring effectiveness of planned activities; and

h) top management should support persons to whom roles and responsibilities relating to information security management have been assigned, so that they are motivated and able to direct and support information security activities within their area.

In cases where the organization implementing and operating an ISMS is part of a larger organization, leadership and commitment can be improved by engagement with the person or group of people that controls and directs the larger organization. If they understand what is involved in implementing an ISMS, they can provide support for top management within the ISMS scope and help them provide leadership and demonstrate commitment to the ISMS. For example, if interested parties outside the scope of the ISMS are engaged in decision making concerning information security objectives and risk criteria and are kept aware of information security outcomes produced by the ISMS, their decisions regarding resource allocations can be aligned to the requirements of the ISMS.

Other information

No other information.

5.2 Policy

Required activity

Top management establishes an information security policy.

Explanation

The information security policy describes the strategic importance of the ISMS for the organization and is available as documented information. The policy directs information security activities in the organization.

The policy states what the needs for information security are in the actual context of the organization.

Guidance

The information security policy should contain brief, high level statements of intent and direction concerning information security. It can be specific to the scope of an ISMS, or can have wider coverage.

All other policies, procedures, activities and objectives related to information security should be aligned to the information security policy.

The information security policy should reflect the organization’s business situation, culture, issues and concerns relating to information security. The extent of the information security policy should be in accordance with the purpose and culture of the organization and should seek a balance between ease of reading and completeness. It is important that users of the policy can identify themselves with the strategic direction of the policy.

The information security policy can either include information security objectives for the organization or describe the framework for how information security objectives are set (i.e. who sets them for the ISMS and how they should be deployed within the scope of the ISMS). For example, in very large organizations, high level objectives should be set by the top management of the entire organization, then, according to a framework established in the information security policy, the objectives should be detailed in a way to give a sense of direction to all interested parties.

The information security policy should contain a clear statement from the top management on its commitment to satisfy information security related requirements.

The information security policy should contain a clear statement that top management supports continual improvement in all activities. It is important to state this principle in the policy, so that persons within the scope of the ISMS are aware of it.

The information security policy should be communicated to all persons within the scope of the ISMS. Therefore, its format and language should be appropriate so that it is easily understandable by all recipients.

Top management should decide to which interested parties the policy should be communicated. The information security policy can be written in such a way that it is possible to communicate it to relevant external interested parties outside of the organization. Examples of such external interested parties are customers, suppliers, contractors, subcontractors and regulators. If the information security policy is made available to external interested parties, it should not include confidential information.

The information security policy may either be a separate standalone policy or included in a comprehensive policy, which covers multiple management system topics within the organization (e.g. quality, environment and information security).

The information security policy should be available as documented information. The requirements in ISO/IEC 27001 do not imply any specific form for this documented information, and therefore is up to the organization to decide what form is most appropriate. If the organization has a standard template for policies, the form of the information security policy should use this template.