BS ISO/IEC 27003:2017

BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of ISO/IEC 27003:2017. It supersedes BS ISO/IEC 27003:2010, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/1, Information Security Management Systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2017

ISBN 978 0 580 83508 7

ICS 03.100.70; 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2017.

Amendments/corrigenda issued since publication

Date	Text affected

BS ISO/IEC 27003:2017

INTERNATIONAL STANDARD

ISO/IEC 27003

Second edition
2017-03-01

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)

COPYRIGHT PROTECTED DOCUMENT

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))."

INTERNATIONAL STANDARD **ISO/IEC 27003:2017(E)**

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 resources 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.

Other information

Further information on policies related to information security can be found in ISO/IEC 27002.

Further information about the relationship between the information security policy and other policies in a policy framework can be found in Annex A.

5.3 Organizational roles, responsibilities and authorities

Required activity

Top management ensures that responsibilities and authorities for roles relevant to information security are assigned and communicated throughout the organization.

Explanation

Top management ensures that roles and responsibilities as well as the necessary authorities relevant to information security are assigned and communicated.

The purpose of this requirement is to assign responsibilities and authorities to ensure conformance of the ISMS with the requirements of ISO/IEC 27001, and to ensure reporting on the performance of the ISMS to the top management.

Guidance

Top management should regularly ensure that the responsibilities and authorities for the ISMS are assigned so that the management system fulfils the requirements stated in ISO/IEC 27001. Top management does not need to assign all roles, responsibilities and authorities, but it should adequately delegate authority to do this. Top management should approve major roles, responsibilities and authorities of the ISMS.

Responsibilities and authorities related to information security activities should be assigned. Activities include:

a) coordinating the establishment, implementation, maintenance, performance reporting, and improvement of the ISMS;

b) advising on information security risk assessment and treatment;

c) designing information security processes and systems;

d) setting standards concerning determination, configuration and operation of information security controls;

e) managing information security incidents; and

f) reviewing and auditing the ISMS.

Beyond the roles specifically related to information security, relevant information security responsibilities and authorities should be included within other roles. For example, information security responsibilities can be incorporated in the roles of:

g) information owners;

h) process owners;

i) asset owners (e.g. application or infrastructure owners);

j) risk owners;

k) information security coordinating functions or persons (this particular role is normally a supporting role in the ISMS);

l) project managers;

m) line managers; and

n) information users.

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.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

Overview

ISO/IEC 27001:2013, 6.1 is concerned with the planning of actions to address all types of risks and opportunities that are relevant to the ISMS. This includes risk assessment and planning for risk treatment.

The structure of ISO/IEC 27001 subdivides risks into two categories during planning:

a) risks and opportunities relevant to the intended outcome(s) of the ISMS as a whole; and

b) information security risks that relate to the loss of confidentiality, integrity and availability of information within the scope of the ISMS.

The first category should be handled in accordance with requirements specified in ISO/IEC 27001:2013, 6.1.1 (general). Risks that fall into this category can be risks relating to the ISMS itself, the ISMS scope definition, top management's commitment to information security, resources for operating the ISMS, etc. Opportunities that fall into this category can be opportunities relating to the outcome(s) of the ISMS, the commercial value of an ISMS, the efficiency of operating ISMS processes and information security controls, etc.

The second category consists of all risks that directly relate to the loss of confidentiality, integrity and availability of information within the scope of the ISMS. These risks should be handled in accordance with 6.1.2 (information security risk assessment) and 6.1.3 (information security risk treatment).

Organizations may choose to use different techniques for each category.

The subdivision of requirements for addressing risks can be explained as follows:

— it encourages compatibility with other management systems standards for those organizations that have integrated management systems for different aspects like quality, environment and information security;

— it requires that the organization defines and applies complete and detailed processes for information security risk assessment and treatment; and

— it emphasizes that information security risk management is the core element of an ISMS.

ISO/IEC 27001:2013, 6.1.1 uses the expressions 'determine the risks and opportunities' and 'address these risks and opportunities'. The word "determine" can be considered to be equivalent to the word "assess" used in ISO/IEC 27001:2013, 6.1.2 (i.e. identify, analyse and evaluate). Similarly, the word "address" can be considered equivalent to the word "treat" used in ISO/IEC 27001:2013, 6.1.3.

Required activity

When planning for the ISMS, the organization determines the risks and opportunities considering issues referred to in 4.1 and requirements referred to in 4.2.

Explanation

For risks and opportunities relevant to the intended outcome(s) of the ISMS, the organization determines them based on internal and external issues (see 4.1) and requirements from interested parties (see 4.2). Then the organization plans its ISMS to:

a) ensure that intended outcomes are delivered by the ISMS, e.g. that the information security risks are known to the risk owners and treated to an acceptable level;

b) prevent or reduce undesired effects of risks relevant to the intended outcome(s) of the ISMS; and

c) achieve continual improvement (see 10.2), e.g. through appropriate mechanisms to detect and correct weaknesses in the management processes or taking opportunities for improving information security.

Risks connected to a) above could be unclear processes and responsibilities, poor awareness among employees, poor engagement from management, etc. Risks connected to b) above could be poor risk management or poor awareness of risks. Risks connected to c) above could be poor management of the ISMS documentation and processes.

When an organization pursues opportunities in its activities, these activities then affect the context of the organization (ISO/IEC 27001:2013, 4.1) or the needs and expectations of interested parties (ISO/IEC 27001:2013, 4.2), and can change the risks to the organization. Examples of such opportunities can be: focusing its business on some areas of products or services, establishing marketing strategy for some geographical regions, or expanding business partnerships with other organizations.

Opportunities also exist in continual improvements of the ISMS processes and documentation, along with evaluation of the intended outcomes delivered by the ISMS. For example, consideration of a relatively new ISMS often results in identification of opportunities to refining processes by clarifying interfaces, reducing administrative overhead, eliminating parts of processes that are not cost effective, by refining documentation and introducing new information technology.

The planning in 6.1.1 includes the determination of:

d) actions to address the risks and opportunities; and

e) the way to:

   1) integrate and implement these actions into the ISMS processes; and

   2) evaluate the effectiveness of these actions.

Guidance

The organization should:

f) determine risks and opportunities that can affect the achievement of the goals described in a), b) and c), considering the issues referred to in 4.1 and the requirements referred to in 4.2; and

g) develop a plan to implement the determined actions and to evaluate the effectiveness of those actions; actions should be planned considering integration of information security processes and documentation in existing structures; all these actions are linked with information security objectives (6.2) against which the information security risks are assessed and treated (see 6.1.2 and 6.1.3).

The general requirement to continually improve the ISMS stated in ISO/IEC 27001:2013, 10.2 is supported by the requirement to achieve continual improvement given in 6.1.1 with other relevant requirements of ISO/IEC 27001:2013, 5.1 g), 5.2 d), 9.1, 9.2 and 9.3.

The actions required in 6.1.1 can be different for strategical, tactical and operational levels, for different sites, or for different services or systems.

Several approaches can be taken to meet the requirements of 6.1.1, two of which are:

— considering risks and opportunities associated with planning, implementing and operating the ISMS separately from information security risks; and

— considering all risks simultaneously.

An organization that is integrating an ISMS into an established management system can find that the requirements of 6.1.1 are met by the organization's existing business planning methodology. Where this is the case, care should be taken to verify that the methodology covers all the requirements of 6.1.1.

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

Further information about risk management can be found in ISO 31000.

NOTE The term "risk" is defined as the "effect of uncertainty on objectives" (see ISO/IEC 27000:2016, 2.68).

6.1.2 Information security risk assessment

Required activity

The organization defines and applies an information security risk assessment process.

Explanation

The organization defines an information security risk assessment process that:

a) establishes and maintains:

   1) the risk acceptance criteria; and

   2) criteria for performing information security risk assessments, which can include criteria for assessing the consequence and likelihood, and rules for the determination of the level of risk; and

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results.

The information security risk assessment process is then defined along the following sub-processes:

c) identification of information security risks:

   1) identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS; and

   2) identify the risk owners associated with these risks, i.e. identify and appoint persons with the appropriate authority and responsibility for managing identified risks.

d) analysis of the information security risks:

   1) assess the potential consequences in case the identified risks materialize, e.g. direct business impacts such as monetary loss or indirect business impacts such as damage in reputation. Assessed consequences can be reported with quantitative or qualitative values;

   2) assess the realistic likelihood of occurrence of the identified risks, with quantitative (i.e. probability or frequency) or qualitative values; and

3) determine the levels of identified risk as a predefined combination of assessed consequences and assessed likelihoods; and

e) evaluation of the information security risks:

1) compare the results of risk analysis with the risk acceptance criteria established before; and

2) prioritize the analysed risks for risk treatment, i.e. determine urgency of treatment for risks that are considered as unacceptable, and sequence if several risks need treatment.

The information security risk assessment process is then applied.

All steps of the information security risk assessment process (6.1.2 a) to e)) as well as the results of its application are retained by the organization as documented information.

Guidance

Guidance on establishing risk criteria (6.1.2 a))

The information security risk criteria should be established considering the context of the organization and requirements of interested parties and should be defined in accordance with top management's risk preferences and risk perceptions on one hand and should allow for a feasible and appropriate risk management process on the other hand.

The information security risk criteria should be established in connection with the intended outcome(s) of the ISMS.

According to ISO/IEC 27001:2013, 6.1.2 a), criteria concerning information security risk assessment that consider the assessment of likelihood and consequences should be established. Further, risk acceptance criteria should be established.

After establishing criteria for assessing consequences and likelihoods of information security risks, the organization should also establish a method for combining them in order to determine a level of risk. Consequences and likelihoods may be expressed in a qualitative, quantitative or semi-quantitative manner.

Risk acceptance criteria relates to risk assessment (in its evaluation phase, when the organization should understand if a risk is acceptable or not), and risk treatment activities (when the organization should understand if the proposed risk treatment is sufficient to reach an acceptable level of risk).

Risk acceptance criteria can be based on a maximum level of acceptable risks, on cost-benefits considerations, or on consequences for the organization.

The risk acceptance criteria should be approved by the responsible management.

Guidance on producing consistent, valid and comparable assessment results (6.1.2 b))

The risk assessment process should be based on methods and tools designed in sufficient detail so that it leads to consistent, valid and comparable results.

Whatever the chosen method, the information security risk assessment process should ensure that:

— all risks, at the needed level of detail, are considered;

— its results are consistent and reproducible (i.e. the identification of risks, their analysis and their evaluation can be understood by a third party and results are the same when different persons assess the risks in the same context); and

— the results of repeated risk assessments are comparable (i.e. it is possible to understand if the levels of risk are increased or decreased).

Inconsistencies or discrepancies in the results when the whole or part of the information security risk assessment process is repeated can indicate that the chosen risk assessment method is not adequate.

Guidance on identification of information security risks (6.1.2 c))

Risk identification is the process of finding, recognizing and describing risks. This involves the identification of risk sources, events, their causes and their potential consequences.

The aim of risk identification is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of information security objectives.

Two approaches are commonly used for the identification of information security risks:

— event-based approach: considers risk sources in a generic way. Events considered can have happened in the past or can be anticipated for the future. In the first case they can involve historical data, in the second case they can be based on theoretical analysis and expert opinions; and

— approach based on identification of assets, threats, and vulnerabilities: considers two different types of risk sources: assets with their intrinsic vulnerabilities, and threats. Potential events considered here are ways as to how threats could exploit a certain vulnerability of an asset to impact the organization's objectives.

Both approaches are consistent with the principles and generic guidelines on risk assessment in ISO 31000.

Other approaches of risk identification may be used if they have proven a similar practical usefulness and if they can ensure the requirements in 6.1.2 b).

NOTE The approach based on assets, threats, and vulnerabilities corresponds to the information security risk identification approach by, and compatible with, the requirements in ISO/IEC 27001 to ensure that previous investments in risk identification are not lost.

It is not recommended that the risk identification be too detailed in the first cycle of risk assessment. Having a high level but clear picture of the information security risks is far better than having no picture at all.

Guidance on analysis of the information security risks (6.1.2 d))

Risk analysis has the objective to determine the level of the risk.

ISO 31000 is referenced in ISO/IEC 27001 as a general model. ISO/IEC 27001 requires that for each identified risk the risk analysis is based on assessing the consequences resulting from the risk and assessing the likelihood of those consequences occurring to determine a level of risk.

Techniques for risk analysis based on consequences and likelihood can be:

1) qualitative, using a scale of qualifying attributes (e.g. high, medium, low);

2) quantitative, using a scale with numerical values (e.g. monetary cost, frequency or probability of occurrence); or

3) semi-quantitative, using qualitative scales with assigned values.

Whatever technique for risk analysis is used, its level of objectivity should be considered.

There are several methods for analysing the risks. The two approaches mentioned (event based approach and approach based on identification of assets, threats, and vulnerabilities) can be suitable for information security risk analysis. Risk identification and analysis processes can be most effective when carried out with the help of experts in the relevant risks under discussion.

Guidance on evaluation of the information security risks (6.1.2 e))

Evaluation of analysed risks involves using the organization's decision making processes to compare the assessed level of risk for each risk with the pre-determined acceptance criteria in order to determine the risk treatment options.

This final step of the risk assessment verifies whether the risks that have been analysed in the previous steps can be accepted according to the acceptance criteria defined under 6.1.2 a), or need further treatment. The step in 6.1.2 d) delivers information about the magnitude of the risk but no immediate information about the urgency of implementing risk treatment options. Depending on the circumstances in which risks occur, they can have different priorities for treatment. Therefore, the output of this step should be a list of risks in priority order. It is useful to retain further information about these risks from the risk identification and risk analysis steps to support decisions for risk treatment.

Other information

ISO/IEC 27005 provides guidance for performing information security risk assessments.

6.1.3 Information security risk treatment

Required activity

The organization defines and applies an information security risk treatment process.

Explanation

Information security risk treatment is the overall process of selecting risk treatment options, determining appropriate controls to implement such options, formulating a risk treatment plan and obtaining approval of the risk treatment plan by the risk owner(s).

All steps of the information security risk treatment process (6.1.3 a) to f)) as well as the results of its application are retained by the organization as documented information.

Guidance

Guidance on information security risk treatment options (6.1.3 a))

Risk treatment options are:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk or by removing the risk source (e.g. closing an e-commerce portal);

b) taking additional risk or increasing risk in order to pursue a business opportunity (e.g. opening an e-commerce portal);

c) modifying the risk by changing the likelihood (e.g. reducing vulnerabilities) or the consequences (e.g. diversifying assets) or both;

d) sharing the risk with other parties by insurance, sub-contracting or risk financing; and

e) retaining the risk based on the risk acceptance criteria or by informed decision (e.g. maintaining the existing e-commerce portal as it is).

Each individual risk should be treated in line with information security objectives by one or more of these options, in order to meet risk acceptance criteria.

Guidance on determining necessary controls (6.1.3 b))

Special attention should be given to the determination of the necessary information security controls. Any control should be determined based on information security risks previously assessed. If an organization has a poor information security risk assessment, it has a poor foundation for its choice of information security controls.

Appropriate control determination ensures:

f) all necessary controls are included, and no unnecessary controls are chosen; and

g) the design of necessary controls satisfies an appropriate breadth and depth.

As a consequence of a poor choice of controls, the proposed information security risk treatment can be:

h) ineffective; or

i) inefficient and therefore inappropriately expensive.

To ensure that information security risk treatment is effective and efficient, it is therefore important to be able to demonstrate the relationship from the necessary controls back to the results of the risk assessment and risk treatment processes.

It can be necessary to use multiple controls to achieve the required treatment of the information security risk. For example, if the option to change the consequences of a particular event is chosen, it may require controls to effect prompt detection of the event as well as controls to respond to and recover from the event.

When determining controls, the organization should also take into account controls needed for services from outside suppliers of e.g. applications, processes and functions. Typically, these controls are mandated by entering information security requirements in the agreements with these suppliers, including ways to get information about to which extent these requirements are met (e.g. right of audit). There may be situations where the organization wishes to determine and describe detailed controls as being part of its own ISMS even though the controls are carried out by outside suppliers. Independently of the approach taken, the organization always should consider controls needed at their suppliers when determining controls for its ISMS.

Guidance on comparing controls with those in ISO/IEC 27001:2013, Annex A (6.1.3 c))

ISO/IEC 27001:2013, Annex A contains a comprehensive list of control objectives and controls. Users of this document are directed to the generic representation of controls in ISO/IEC 27001:2013, Annex A to ensure that no necessary controls are overlooked. Comparison with ISO/IEC 27001:2013, Annex A can also identify alternative controls to those determined in 6.1.3 b) which can be more effective at modifying information security risk.

Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in ISO/IEC 27001:2013, Annex A are not exhaustive and additional control objectives and controls should be added as needed.

Not every control within ISO/IEC 27001:2013, Annex A needs to be included. Any control within ISO/IEC 27001:2013, Annex A that does not contribute to modifying risk should be excluded and justification for the exclusion should be given.

Guidance on producing a Statement of Applicability (SoA) (6.1.3 d))

The SoA contains:

— all necessary controls (as determined in 6.1.3 b) and 6.1.3 c)) and, for each control:

  — the justification for the control's inclusion; and

  — whether the control is implemented or not (e.g. fully implemented, in progress, not yet started); and

— the justification for excluding any of the controls in ISO/IEC 27001: 2013, Annex A.

Justification for including a control in part relies on the effect of the control in modifying an information security risk. A reference to information security risk assessment results and the information security risk treatment plan should be sufficient, along with the information security risk modification expected by the implementation of necessary controls.

Justification for excluding a control contained within ISO/IEC 27001:2013, Annex A can include the following:

— it has been determined that the control is not necessary to implement the chosen information security risk treatment option(s);

— the control is not applicable because it is outside the scope of the ISMS (e.g. ISO/IEC 27001:2013, A.14.2.7 Outsourced development is not applicable if all the organization's system development is performed in-house); and

— it is obviated by a custom control (e.g. in ISO/IEC 27001:2013, A.8.3.1 management of removable media could be excluded if a custom control prevents the use of removable media).

NOTE A custom control is a control not included in ISO/IEC 27001:2013, Annex A.

A useful SoA can be produced as a table containing all 114 controls of ISO/IEC 27001:2013, Annex A along the rows plus rows with the additional controls that are not mentioned in ISO/IEC 27001:2013, Annex A, if needed. One column of the table can indicate whether a control is necessary to implement the risk treatment option(s) or can be excluded. A next column can contain the justification for inclusion or exclusion of a control. A last column of the table can indicate the current implementation status of the control. Further columns can be used, such as for details not required by ISO/IEC 27001 but usually useful for subsequent reviews; these details can be a more detailed description of how the control is implemented or a cross-reference to a more detailed description and documented information or policies relevant for implementing the control.

Although it is not a specific requirement of ISO/IEC 27001, organizations can find it useful to include responsibilities for the operation of each control included in the SoA.

Guidance on formulating an information security risk treatment plan (6.1.3 e))

ISO/IEC 27001 does not specify a structure or content for the information security risk treatment plan. However, the plan should be formulated from the outputs of 6.1.3 a) to c). Thus the plan should document for each treated risk:

— selected treatment option(s);

— necessary control(s); and

— implementation status.

Other useful content can include:

— risk owner(s); and

— expected residual risk after the implementation of actions.

If any action is required by the risk treatment plan, then it should be planned indicating responsibilities and deadlines (see also 6.2); such an action plan can be represented by a list of these actions.

A useful information security risk treatment plan can be designed as a table sorted by risks identified during the risk assessment, showing all the determined controls. As an example, there can be columns in this table which indicate the names of the persons responsible for providing the controls. Further columns can indicate the date of implementation of the control, information about how the control (or a process) is intended to operate and a column about the target implementation status.

As an example for part of the risk treatment process, consider the theft of a mobile phone. The consequences are loss of availability and potential undesirable disclosure of information. If the assessment of the risk showed that the level of risk is out of acceptance, the organization can decide to change the likelihood, or change the consequences of the risk.

To change the likelihood of loss or theft of a mobile phone, the organization can determine that a suitable control is to oblige employees through a mobile device policy to take care of mobile phones and periodically check for loss.

To change the consequence of loss or theft of a mobile phone, the organization can determine controls such as:

— an incident management process so users can report the loss;

— a Mobile Device Management (MDM) solution to delete the content of the phone if lost; and

— a backup plan of mobile devices for recovering the phone's content.

When preparing its SoA (6.1.3 d)), the organization can include its chosen controls (mobile device policy and MDM), justifying their inclusion based on their effect of changing the likelihood and consequences of mobile phone loss or theft, resulting in reduced residual risk.

Comparing these controls with those listed in ISO/IEC 27001:2013, Annex A (6.1.3 c)), it can be seen that the mobile device policy is aligned with ISO/IEC 27001:2013, A.6.2.1, but the MDM control does not directly align and should be considered as an additional custom control. If MDM and other controls are determined as necessary control(s) in an organization's information security risk treatment plan, they should be included in the SoA (see "Guidance on producing an SoA (6.1.3 d)).

If the organization wants to further reduce the risk, it can consider from ISO/IEC 27001:2013, A.9.1.1 (access control policy) that it lacked control of access to mobile phones and modify its mobile device policy to mandate the use of PINs on all mobile phones. This should then be a further control to change the consequences of loss or theft of mobile phones.

When formulating its information security risk treatment plan (6.1.3 e)), the organization should then include actions to implement mobile device policy and MDM and assign responsibilities and timeframes.

Guidance on obtaining risk owners' approval (6.1.3 f))

When the information security risk treatment plan is formulated, the organization should obtain the authorization from the risk owners. Such authorization should be based on defined risk acceptance criteria or justified concession if there is any deviance from them.

Through its management processes the organization should record the risk owner's acceptance of the residual risk and management approval of the plan.

As an example, this risk owner's approval can be documented by amending the risk treatment plan described under guidance on 6.1.3 e) by columns indicating the effectiveness of the control, the residual risk, and the risk owner's approval.

Other information

Further information on risk treatment can be found in ISO/IEC 27005 and ISO 31000.

6.2 Information security objectives and planning to achieve them

Required activity

The organization establishes information security objectives and plans to achieve them at relevant functions and levels.

Explanation

Information security objectives help to implement strategic goals of an organization as well as to implement the information security policy. Thereby, objectives in an ISMS are the information security objectives for confidentiality, integrity and availability of information. Information security objectives also help to specify and measure the performance of information security controls and processes, in accordance with the information security policy (see 5.2).

The organization plans, establishes and issues information security objectives to relevant functions and levels.

Requirements in ISO/IEC 27001 concerning information security objectives apply to all information security objectives. If the information security policy contains objectives, then those objectives are required to meet the criteria in 6.2. If the policy contains a framework for setting objectives, then the objectives produced by that framework are required to meet the requirements of 6.2.

Requirements to be taken into account when establishing objectives are those determined when understanding the organisation and its context (see 4.1) as well as the needs and expectations of interested parties (see 4.2).

The results from risk assessments and risk treatments are used as input to the on-going review of objectives to ensure that they remain appropriate to the circumstances of an organization.

Information security objectives are inputs for risk assessment: risk acceptance criteria and criteria for performing information security risk assessments (see 6.1.2) take into account these information security objectives and thus ensure that levels of risk are aligned with them.

Information security objectives as per ISO/IEC 27001 are:

a) consistent with the information security policy;

b) measurable if practicable; this means that it is important to be able to determine whether or not an objective has been met;

c) connected to applicable information security requirements, and results from risk assessment and risk treatment;

d) communicated; and

e) updated as appropriate.

The organization retains documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization determines:

f) what will be done;

g) what resources will be required;

h) who will be responsible;

i) when it will be completed; and

j) how the results will be evaluated.

The above requirement concerning planning is generic and applicable to other plans required by ISO/IEC 27001. Plans to consider for an ISMS include:

— plans for improving the ISMS as described in 6.1.1 and 8.1;

— plans for treating identified risks as described in 6.1.3 and 8.3; and

— any other plans that are found necessary for effective operation (e.g. plans for developing competence and increasing awareness, communication, performance evaluation, internal audits and management reviews).

Guidance

The information security policy should state the information security objectives or provide a framework for setting the objectives.

Information security objectives can be expressed in various ways. The expression should be suitable to meet the requirement of being measurable (if practicable) (ISO/IEC 27001:2013, 6.2 b)).

For example, information security objectives can be expressed in terms of:

— numerical values with their limits, e.g. “not go over a certain limit”, and “reach level 4”;

— the targets for measurements of information security performance;

— the targets for measurements of the effectiveness of the ISMS (see 9.1);

— compliance with ISO/IEC 27001;

— compliance with ISMS procedures;

— the need to complete actions and plans; and

— risk criteria to be met.

The following guidance applies to the bullets addressed in the explanation:

— see a) above. The information security policy specifies the requirements for information security in an organization. All other specific requirements set for relevant functions and levels should be consistent with them. If the information security policy has information security objectives, then any other specific information security objective should be linked to the ones in the information security policy. If the information security policy only provides the framework for setting objectives, then that framework should be followed and should ensure that more specific objectives are linked to the more generic ones;

— see b) above. Not every objective can be measurable, but making objectives measurable supports achievement and improvement. It is highly desirable to be able to describe, qualitatively or quantitatively, the degree to which an objective has been met. For example, to guide priorities for additional effort if objectives are not met, or to provide insights into opportunities for improved effectiveness if objectives are exceeded. It should be possible to understand whether they have been achieved or not, how achievement of objectives is determined, and whether it is possible to determine the degree of achievement of objectives using quantitative measurements. Quantitative descriptions of objective attainment should specify how associated measurement is done. It may not be possible to quantitatively determine the degree of attainment of all objectives. ISO/IEC 27001 requires objectives to be measurable if practicable;

— see c) above. Information security objectives should be aligned with information security needs; for this reason, risk assessment and treatment results should be used as inputs when setting information security objectives;

— see d) above. Information security objectives should be communicated to relevant internal interested parties of the organization. They may also be communicated to external interested parties, e.g. customers, stakeholders, to the extent they need to know and are affected by the information security objectives; and

— see e) above. When information security needs change over time, related information security objectives should be updated accordingly. Their update should be communicated as required in d), to internal and external interested parties as appropriate.

The organization should plan how to achieve its information security objectives. The organisation may use any methodology or mechanism it chooses to plan for the achievement of its information security objectives. There may be a single information security plan, one or more project plans, or actions included in other organisational plans. Whatever form planning takes, the resulting plans should define as a minimum (see f) to j) above):

— the activities to be done;

— the required resources to be committed to execute the activities;

— the responsibilities;

— the timelines and milestones of activities; and

— the methods and measurements to evaluate whether the results achieve objectives, which includes timing of such evaluations.

ISO/IEC 27001 requires organizations to retain documented information on the information security objectives. Such documented information can include:

— plans, actions, resources, responsibilities, deadlines and evaluation methods; and

— requirements, tasks, resources, responsibilities, evaluation frequency and methods.

Other information

No other information.

7 Support

7.1 Resources

Required activity

The organization determines and provides the resources for establishing, implementing, maintaining and continually improving the ISMS.

Explanation

Resources are fundamental to perform any kind of activity. Categories of resources can include:

a) persons to drive and operate the activities;

b) time to perform activities and time to allow results to settle down before making a new step;

c) financial resources to acquire, develop and implement what is needed;

d) information to support decisions, measure performance of actions, and improve knowledge; and

e) infrastructure and other means that can be acquired or built, such as technology, tools and materials, regardless of whether they are products of information technology or not.

These resources are to be kept aligned with the needs of the ISMS and hence are to be adapted when required.

Guidance

The organization should:

f) estimate the resources needed for all the activities related to the ISMS in terms of quantity and quality (capacities and capabilities);

g) acquire the resources as needed;

h) provide the resources;

i) maintain the resources across the whole ISMS processes and specific activities; and

j) review the provided resources against the needs of the ISMS, and adjust them as required.

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

No other information.

7.2 Competence

Required activity

The organization determines the competence of persons needed for information security performance, and ensures that the persons are competent.

Explanation

Competence is the ability to apply knowledge and skills to achieve intended results. It is influenced by knowledge, experience and wisdom.

Competence can be specific (e.g. about technology or specific management areas such as risk management) or general (e.g. soft skills, trustworthiness, and basic technological and managerial subjects).

Competence relates to persons that work under control of the organization. This means that competence should be managed for persons that are employees of the organization and for other people as needed.

Acquisition of higher or new competence and skills can be achieved both internally and externally through experience, training (e.g. courses, seminars and workshops), mentoring, hiring or contracting external persons.

For competence that is only temporarily needed – for a specific activity or for a short period of time, e.g. to cover unexpected temporary shortage of internal personnel – organizations can hire or contract external resources, whose competence is to be described and verified.

Guidance

The organization should:

a) determine the expected competence for each role within the ISMS and decide if it needs to be documented (e.g. in a job description);

b) assign the roles within the ISMS (see 5.3) to persons with the required competence either by:

   1) identifying persons within the organization who have the competence (based e.g. on their education, experience, or certifications);

   2) planning and implementing actions to have persons within the organization obtain the competence (e.g. through provision of training, mentoring, reassignment of current employees); or

   3) engaging new persons who have the competence (e.g. through hiring or contracting);

c) evaluate the effectiveness of actions in b) above;

EXAMPLE 1 Consider if persons have acquired competence after the training.

EXAMPLE 2 Analyse the competence of newly hired or contracted persons some time after their arrival in the organization.

EXAMPLE 3 Verify if the plan for acquiring new persons has been completed as expected.

d) verify that the persons are competent for their roles; and

e) ensure that the competence evolves over time as necessary and that it meets expectations.

Appropriate documented information is required as evidence of competence. The organization should therefore retain documentation about the necessary competence affecting information security performance and how this competence is met by relevant persons.

Other information

No other information.

7.3 Awareness

Required activity

The persons doing work under the organization's control are made aware of the information security policy, their contribution to the effectiveness of the ISMS, benefits of improved information security performance and implications of not conforming to the requirements of the ISMS.

Explanation

Awareness of persons working under the organization's control refers to having the necessary understanding and motivation about what is expected of them with regard to information security.

Awareness concerns persons who have to know, understand, accept and:

a) support the objectives stated in the information security policy; and

b) follow the rules to correctly perform their daily tasks in support of information security.

Additionally, the persons doing work under the organization's control also need to know, understand and accept the implications of not conforming with the ISMS requirements. Implications can be negative consequences for information security or repercussions for the person.

These persons need to be aware that an information security policy exists and where to find information about it. Many staff in an organization do not need to know the detailed content of the policy. Instead, they should know, understand, accept and implement the information security objectives and requirements derived from the policy that affect their job role. These requirements can be included in the standards or procedures they are expected to follow to do their job.

Guidance

The organization should:

c) prepare a programme with the specific messages focused on each audience (e.g. internal and external persons);

d) include information security needs and expectations within awareness and training materials on other topics to place information security needs into relevant operational contexts;

e) prepare a plan to communicate messages at planned intervals;

f) verify the knowledge and understanding of messages both at the end of an awareness session and at random between sessions; and

g) verify whether persons act according to the communicated messages and use examples of 'good' and 'bad' behaviour to reinforce the message.

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

Further information on awareness in the field of information security can be found in ISO/IEC 27002:2013, 7.2.2.

7.4 Communication

Required activity

The organization determines the needs for internal and external communications related to the ISMS.

Explanation

Communication is a key process within an ISMS. Adequate communication is necessary with internal and external interested parties (see 4.2).

Communication can be between internal interested parties at all levels of the organization or between the organization and external interested parties. Communication can be initiated within the organization or by an external interested party.

Organizations need to determine:

— which content needs to be communicated, e.g. information security policies, objectives, procedures, their changes, knowledge on information security risks, requirements to suppliers and feedback on the information security performance;

— the preferred or optimal point in time for communication activities;

— who is to be involved in communication activities, and which is the target audience of each communication effort;

— who is to initiate communication activities, e.g. specific content can require communication to be initiated by a specific person or organization; and

— which processes are driving or initiating communication activities, and which processes are targeted or affected by communication activities.

Communication can take place regularly or as needs arise. It can be either proactive or reactive.

Guidance

Communication relies on processes, channels and protocols. These should be chosen to ensure the communicated message is integrally received, correctly understood and, when relevant, acted upon appropriately.

Organizations should determine which content needs to be communicated, such as:

a) plans and results of risk management to interested parties as needed and appropriate, in the identification, analysis, evaluation, and treatment of the risks;

b) information security objectives;

c) achieved information security objectives including those that can support their position in the market (e.g. ISO/IEC 27001 certificate granted; claiming conformance with personal data protection laws);

d) incidents or crises, where transparency is often key to preserve and increase trust and confidence in the organization's capability to manage its information security and deal with unexpected situations;

e) roles, responsibilities and authority;

f) information exchanged between functions and roles as required by the ISMS's processes;

g) changes to the ISMS;

h) other matters identified by reviewing the controls and processes within the scope of the ISMS;

i) matters (e.g. incident or crisis notification) that require communication to regulatory bodies or other interested parties; and

j) requests or other communications from external parties such as customers, potential customers, users of services and authorities.

The organization should identify the requirements for communication on relevant issues:

k) who is allowed to communicate externally and internally (e.g. in special cases such as a data breach), allocating to specific roles with the appropriate authority. For example, official communication officers can be defined with the appropriate authority. They could be a public relations officer for external communication and a security officer for internal communication;

l) the triggers or frequency of communication (e.g. for communication of an event, the trigger is the identification of the event);

m) the contents of messages for key interested parties (e.g. customers, regulators, general public, important internal users) based on high level impact scenarios. Communication can be more effective if based on messages prepared and pre-approved by an appropriate level of management as part of a communication plan, the incident response plan or the business continuity plan;

n) the intended recipients of the communication; in some cases, a list should be maintained (e.g. for communicating changes to services or crisis);

o) the communication means and channels. Communication should use dedicated means and channels, to make sure that the message is official and bears the appropriate authority. Communication channels should address any needs for the protection of the confidentiality and integrity of the information transmitted; and

p) the designed process and the method to ensure messages are sent and have been correctly received and understood.

Communication should be classified and handled according to the organization's requirements.

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.

7.5 Documented information

7.5.1 General

Required activity

The organization includes documented information in the ISMS as directly required by ISO/IEC 27001, as well as determined by the organization as being necessary for the effectiveness of the ISMS.

Explanation

Documented information is needed to define and communicate information security objectives, policy, guidelines, instructions, controls, processes, procedures, and what persons or groups of people are expected to do and how they are expected to behave. Documented information is also needed for audits of the ISMS and to maintain a stable ISMS when persons in key roles change. Further, documented information is needed for recording actions, decisions and outcome(s) of ISMS processes and information security controls.

Documented information can contain:

— information about information security objectives, risks, requirements and standards;

— information about processes and procedures to be followed; and

— records of the input (e.g. for management reviews) and the outcomes of processes (including plans and outcomes of operational activities).

There are many activities within the ISMS that produce documented information that is used, most of the time, as an input for another activity.

ISO/IEC 27001 requires a set of mandatory documented information and contains a general requirement that additional documented information is required if it is necessary for the effectiveness of the ISMS.

The amount of documented information needed is often related to the size of the organization.

In total, the mandatory and additional documented information contains sufficient information to allow the performance evaluation requirements specified in Clause 9 to be carried out.

Guidance

The organization should determine what documented information is necessary for ensuring effectiveness of its ISMS in addition to mandatory documented information required by ISO/IEC 27001.

The documented information should be there to fit the purpose. Factual and 'to the point' information is what is needed.

Examples of documented information that can be determined by the organization to be necessary for ensuring effectiveness of its ISMS are:

— the results of the context establishment (see Clause 4);

— the roles, responsibilities and authorities (see Clause 5);

— reports of the different phases of the risk management (see Clause 6);

— resources determined and provided (see 7.1);

— the expected competence (see 7.2);

— plans and results of awareness activities (see 7.3);

— plans and results of communication activities (see 7.4);

— documented information of external origin that is necessary for the ISMS (see 7.5.3);

— process to control documented information (see 7.5.3);

— policies, rules and directives for directing and operating information security activities;

— processes and procedures used to implement, maintain and improve the ISMS and the overall information security status (see Clause 9);

— action plans; and

— evidence of the results of ISMS processes (e.g. incident management, access control, information security continuity, equipment maintenance, etc.).

Documented information can be of internal or external origin.

Other information

If the organization wants to manage its documented information in a document management system, this can be built according to the requirements in ISO 30301.

7.5.2 Creating and updating

Required activity

When creating and updating documented information, the organization ensures its appropriate identification and description, format and media, and review and approval.

Explanation

The organization identifies in detail how the documented information is best structured and defines a suitable documentation approach.

Review and approval by appropriate management ensures that the documented information is correct, suitable for the purpose, and in an adequate form and detail for the intended audience. Regular reviews ensure continued suitability and adequacy of documented information.

Guidance

Documented information may be retained in any form, e.g. traditional documents (in both paper and electronic form), web pages, databases, computer logs, computer generated reports, audio and video. Moreover, documented information may consist of specifications of intent (e.g. the information security policy) or records of performance (e.g. the results of an audit) or a mixture of both. The following guidance applies directly to traditional documents and should be interpreted appropriately when applied to other forms of documented information.

Organizations should create a structured documented information library, linking different parts of documented information by:

a) determining the structure of the documented information framework;

b) determining the standard structure of the documented information;

c) providing templates for different types of documented information;

d) determining the responsibilities for preparing, approving, publishing and managing the documented information; and

e) determining and documenting the revision and approval process to ensure continual suitability and adequacy.

Organizations should define a documentation approach that includes common attributes of every document, which allow clear and unique identification. These attributes usually include document type (e.g. policy, directive, rule, guideline, plan, form, process or procedure), the purpose and scope, title, date of publication, classification, reference number, version number, and a revision history. The identification of the author and the person(s) currently responsible for the document, its application and evolution, as well as the approver(s) or approval authority should be included.

Format requirements can include definition of suitable documentation languages, file formats, software version for working with them and graphical content. Media requirements define on which physical and electronic media the information should be available.

Statements and writing style should be tailored to the audience and scope of the documentation.

Duplication of information in documented information should be avoided and cross-references used rather than replicating the same information in different documents.

The documentation approach should ensure timely review of the documented information and that all documentation changes are subject to approval. Suitable review criteria can be timing related (e.g. maximum time periods between document reviews) or content related. Approval criteria should be defined, which ensures that the documented information is correct, suitable for the purpose, and in an adequate form and detail for the intended audience.

Other information

No other information.

7.5.3 Control of documented information

Required activity

The organization manages documented information throughout its lifecycle and makes it available where and when needed.

Explanation

Once approved, the documented information is communicated to its intended audience. Documented information is available where and when it is needed, while preserving its integrity, confidentiality, and relevance throughout the whole lifecycle.

Note that activities described "as applicable" in ISO/IEC 27001:2013, 7.5.3 need to be performed if they can be performed and are useful, considering the organization's needs and expectations.

Guidance

A structured documented information library can be used to facilitate access to documented information.

All of the documented information should be classified (see ISO/IEC 27001:2013, A.8.2.1) in accordance with the organization's classification scheme. Documented information should be protected and handled in accordance with its classification level (see ISO/IEC 27001:2013, A.8.2.3).

A change management process for documented information should ensure that only authorised persons have the right to change and distribute it as needed through appropriate and predefined means. Documented information should be protected to ensure it keeps its validity and authenticity.

Documented information should be distributed and made available to authorized interested parties. For this, the organization should establish who are the relevant interested parties for each documented information (or groups of documented information), and the means to use for distribution, access, retrieval and use (e.g. a web site with appropriate access control mechanisms). The distribution should comply with any requirements related to protecting and handling of classified information.

The organization should establish the appropriate retention period for documented information according to its intended validity and other relevant requirements. The organization should ensure that information is legible throughout its retention period (e.g. using formats that can be read by available software, or verifying that paper is not corrupted).

The organization should establish what to do with documented information after its retention period has expired.

The organization should also manage documented information of external origin (i.e. from customers, partners, suppliers, regulatory bodies, etc.).

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.

8 Operation

8.1 Operational planning and control

Required activity

The organization plans, implements and controls the processes to meet its information security requirements and to achieve its information security objectives.

The organization keeps documented information as necessary to have confidence that processes are carried out as planned.

The organization controls planned changes and reviews the consequences of unintended changes, and ensures that outsourced processes are identified, defined and controlled.

Explanation

The processes that an organization uses to meet its information security requirements are planned, and once implemented, they are controlled, particularly when changes are required.

Building on the planning of the ISMS (see 6.1 and 6.2), the organization performs the necessary operational planning and activities to implement the processes needed to fulfil the information security requirements.

Processes to meet information security requirements include:

a) ISMS processes (e.g. management review, internal audit); and

b) processes required for implementing the information security risk treatment plan.

Implementation of plans results in operated and controlled processes.

The organization ultimately remains responsible for planning and controlling any outsourced processes in order to achieve its information security objectives. Thus the organization needs to:

c) determine outsourced processes considering the information security risks related to the outsourcing; and

d) ensure that outsourced processes are controlled (i.e. planned, monitored and reviewed) in a manner that provides assurance that they operate as intended (also considering information security objectives and the information security risk treatment plan).

After the implementation is completed, the processes are managed, monitored and reviewed to ensure that they continue to fulfil the requirements determined after understanding the needs and expectations of interested parties (see 4.2).

Changes of the ISMS in operation can be either planned or they occur unintended. Whenever the organization makes changes to the ISMS (as a result of planning or unintentionally), it assesses the potential consequences of the changes to control any adverse effects.

The organization can get confidence about the effectiveness of the implementation of plans by documenting activities and using documented information as input to the performance evaluation processes specified in Clause 9. The organization therefore establishes the required documented information to keep.

Guidance

The processes that have been defined as a result of the planning described in Clause 6 should be implemented, operated and verified throughout the organization. The following should be considered and implemented:

e) processes that are specific for the management of information security (such as risk management, incident management, continuity management, internal audits, management reviews);

f) processes emanating from information security controls in the information security risk treatment plan;

g) reporting structures (contents, frequency, format, responsibilities, etc.) within the information security area, for example incident reports, reports on measuring the fulfilment of information security objectives, reports on performed activities; and

h) meeting structures (frequency, participants, purpose and authorization) within the information security area. Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions for effective management of the information security area.

For planned changes, the organization should:

i) plan their implementation and assign tasks, responsibilities, deadlines and resources;

j) implement changes according to the plan;

k) monitor their implementation to confirm that they are implemented according to the plan; and

l) collect and retain documented information on the execution of the changes as evidence that they have been carried out as planned (e.g. with responsibilities, deadlines, effectiveness evaluations).

For observed unintended changes, the organization should:

m) review their consequences;

n) determine whether any adverse effects have already occurred or can occur in the future;

o) plan and implement actions to mitigate any adverse effects as necessary; and

p) collect and retain documented information on unintended changes and actions taken to mitigate adverse effects.

If part of the organization's functions or processes are outsourced to suppliers, the organization should:

q) determine all outsourcing relationships;

r) establish appropriate interfaces to the suppliers;

s) address information security related issues in the supplier agreements;

t) monitor and review the supplier services to ensure that they are operated as intended and associated information security risks meet the risk acceptance criteria of the organization; and

u) manage changes to the supplier services as necessary.

Other information

No other information.

8.2 Information security risk assessment

Required activity

The organization performs information security risk assessments and retains documented information on their results.

Explanation

When performing information security risk assessments, the organization executes the process defined in 6.1.2. These assessments are either executed according to a schedule defined in advance, or in response to significant changes or information security incidents. The results of the information security risk assessments are retained in documented information as evidence that the process in 6.1.2 has been performed as defined.

Documented information from information security risk assessments is essential for information security risk treatment and is valuable for performance evaluation (see Clause 9).

Guidance

Organizations should have a plan for conducting scheduled information security risk assessments.

When any significant changes of the ISMS (or its context) or information security incidents have occurred, the organization should determine:

a) which of these changes or incidents require an additional information security risk assessment; and

b) how these assessments are triggered.

The level of detail of the risk identification should be refined step by step in further iterations of the information security risk assessment in the context of the continual improvement of the ISMS. A broad information security risk assessment should be performed at least once a year.

Other information

ISO/IEC 27005 provides guidance for performing information security risk assessments.

8.3 Information security risk treatment

Required activity

The organization implements the information security risk treatment plan and retains documented information on the results of the information security treatment.

Explanation

In order to treat information security risks, the organization needs to carry out the information security risk treatment process defined in 6.1.3. During operation of the ISMS, whenever the risk assessment is updated according to 8.2, the organization then applies the risk treatment according to 6.1.3 and updates the risk treatment plan. The updated risk treatment plan is again implemented.

The results of the information security risk treatment are retained in documented information as evidence that the process in 6.1.3 has been performed as defined.

Guidance

The information security risk treatment process should be performed after each iteration of the information security assessment process in 8.2 or when the implementation of the risk treatment plan or parts of it fails.

The progress of implementation of the information security risk treatment plan should be driven and monitored by this activity.

Other information

No other information.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

Required activity

The organization evaluates the information security performance and the effectiveness of the ISMS.

Explanation

The objective of monitoring and measurement is to help the organization to judge whether the intended outcome of information security activities including risk assessment and treatment is achieved as planned.

Monitoring determines the status of a system, a process or an activity, whilst measurement is a process to determine a value. Thus monitoring can be achieved through a succession of similar measurements over some time period.

For monitoring and measurement, the organization establishes:

a) what to monitor and measure;

b) who monitors and measures, and when; and

c) methods to be used so as to produce valid results (i.e. comparable and reproducible).

For analysis and evaluation, the organization establishes:

d) who analyses and evaluates the results from monitoring and measurement, and when; and

e) methods to be used so as to produce valid results.

There are two aspects of evaluation:

f) evaluating the information security performance, for determining whether the organization is doing as expected, which includes determining how well the processes within the ISMS meet their specifications; and

g) evaluating the effectiveness of the ISMS, for determining whether or not the organization is doing the right things, which includes determining the extent to which information security objectives are achieved.

Note that as “as applicable” (ISO/IEC 27001:2013, 9.1, b)) means that if methods for monitoring, measurement, analysis and evaluation can be determined, they need to be determined.

Guidance

A good practice is to define the ‘information need’ when planning the monitoring, measurement, analysis and evaluation. An information need is usually expressed as a high level information security question or statement that helps the organization evaluate information security performance and ISMS effectiveness. In other words, monitoring and measurement should be undertaken to achieve a defined information need.

Care should be taken when determining the attributes to be measured. It is impracticable, costly and counterproductive to measure too many, or the wrong attributes. Besides the costs of measuring, analysing and evaluating numerous attributes, there is a possibility that key issues could be obscured or missed altogether.

There are two generic types of measurements:

h) **performance measurements**, which express the planned results in terms of the characteristics of the planned activity, such as head counts, milestone accomplishment, or the degree to which information security controls are implemented; and

i) **effectiveness measurements**, which express the effect that realization of the planned activities has on the organization's information security objectives.

It can be appropriate to identify and assign distinctive roles to those participating in the monitoring, measurement, analysis and evaluation. Those roles can be measurement client, measurement planner, measurement reviewer, information owner, information collector, information analyst and information communicator of input or output of evaluation (see ISO/IEC 27004:2016, 6.5).

The responsibilities for monitoring and measurement and those for analysis and evaluation are often assigned to separate persons whom different competence is required.

Other information

Monitoring, measurement, analysis and evaluation is critical to the success of an effective ISMS. There are a number of clauses in ISO/IEC 27001 that explicitly require determination of the effectiveness of some activities. For example, ISO/IEC 27001:2013, 6.1.1 e), 7.2 c) or 10.1 d).

Further information can be found in ISO/IEC 27004, which provides guidance on meeting the requirements of ISO/IEC 27001:2013, 9.1. In particular, it expands on all of the concepts mentioned above, such as roles and responsibilities, and forms, and gives numerous examples.

9.2 Internal audit

Required activity

The organization conducts internal audits to provide information on conformity of the ISMS to the requirements.

Explanation

Evaluating an ISMS at planned intervals by means of internal audits provides assurance of the status of the ISMS to top management. Auditing is characterized by a number of principles: integrity; fair presentation; due professional care; confidentiality; independence; and evidence-based approach (see ISO 19011).

Internal audits provide information on whether the ISMS conforms to the organization's own requirements for its ISMS as well as to the requirements in ISO/IEC 27001. The organization's own requirements include:

a) requirements stated in the information security policy and procedures;

b) requirements produced by the framework for setting information security objectives, including outcomes of the risk treatment process;

c) legal and contractual requirements; and

d) requirements on the documented information.

Auditors also evaluate whether the ISMS is effectively implemented and maintained.

An audit programme describes the overall framework for a set of audits, planned for specific time frames and directed towards specific purposes. This is different from an audit plan, which describes the activities and arrangements for a specific audit. Audit criteria are a set of policies, procedures or requirements used as a reference against which audit evidence is compared, i.e. the audit criteria describe what the auditor expects to be in place.

An internal audit can identify nonconformities, risks and opportunities. Nonconformities are managed according to requirements in 10.1. Risks and opportunities are managed according to requirements in 4.1 and 6.1.

The organization is required to retain documented information about audit programme(s) and audit results.

Guidance

Managing an audit programme

An audit programme defines the structure and responsibilities for planning, conducting, reporting and following up on individual audit activities. As such it should ensure that audits conducted are appropriate, have the right scope, minimize the impact on the operations of the organization and maintain the necessary quality of audits. An audit programme should also ensure the competence of audit teams, appropriate maintenance of audit records, and the monitoring and review of the operations, risks and effectiveness of audits. Further, an audit programme should ensure that the ISMS (i.e. all relevant processes, functions and controls) is audited within a specified time frame. Finally, an audit programme should include documented information about types, duration, locations, and schedule of the audits.

The extent and frequency of internal audits should be based on the size and nature of the organization as well as on the nature, functionality, complexity and the level of maturity of the ISMS (risk-based auditing).

The effectiveness of the implemented controls should be examined within the scope of internal audits. An audit programme should be designed to ensure coverage of all necessary controls and should include evaluation of the effectiveness of selected controls over time. Key controls (according to the audit programme) should be included in every audit whereas controls implemented to manage lower risks may be audited less frequently.

The audit programme should also consider that processes and controls should have been in operation for some time to enable evaluation of suitable evidence.

Internal audits concerning an ISMS can be performed effectively as a part of, or in collaboration with, other internal audits of the organization. The audit programme can include audits related to one or more management system standards, conducted either separately or in combination.

An audit programme should include documented information about: audit criteria, audit methods, selection of audit teams, processes for handling confidentiality, information security, health and safety provisions for auditors, and other similar matters.

Competence and evaluation of auditors

Regarding competence and evaluation of auditors, the organization should:

e) identify competence requirements for its auditors;

f) select internal or external auditors with the appropriate competence;

g) have a process in place for monitoring the performance of auditors and audit teams; and

h) include personnel on internal audit teams that have appropriate sector specific and information security knowledge.

Auditors should be selected considering that they should be competent, independent, and adequately trained.

Selecting internal auditors can be difficult for smaller companies. If the necessary resources and competence are not available internally, external auditors should be appointed. When organizations use external auditors, they should ensure that they have acquired enough knowledge about the context of the organization. This information should be supplied by internal staff.

Organizations should consider that internal employees acting as internal auditors can be able to perform detailed audits considering the organization's context, but may not have enough knowledge about performing audits.

Organizations should then recognize characteristics and potential shortcomings of internal versus external auditors and establish suitable audit teams with the necessary knowledge and competence.

Performing the audit

When performing the audit, the audit team leader should prepare an audit plan considering results of previous audits and the need to follow up on previously reported nonconformities and unacceptable risks. The audit plan should be retained as documented information and should include criteria, scope and methods of the audit.

The audit team should review:

— adequacy and effectiveness of processes and determined controls;

— fulfilment of information security objectives;

— compliance with requirements defined in ISO/IEC 27001:2013, Clauses 4 to 10;

— compliance with the organization's own information security requirements;

— consistency of the Statement of Applicability against the outcome of the information security risk treatment process;

— consistency of the actual information security risk treatment plan with the identified assessed risks and the risk acceptance criteria;

— relevance (considering organization's size and complexity) of management review inputs and outputs; and

— impacts of management review outputs (including improvement needs) on the organization.

The extent and reliability of available monitoring over the effectiveness of controls as produced by the ISMS (see 9.1) may allow the auditors to reduce their own evaluation efforts, provided they have confirmed the effectiveness of the measurement methods.

If the outcome of the audit includes nonconformities, the auditee should prepare an action plan for each nonconformity to be agreed with the audit team leader. A follow-up action plan typically includes:

i) description of the detected nonconformity;

j) description of the cause(s) of nonconformity;

k) description of short term correction and longer term corrective action to eliminate a detected nonconformity within a defined timeframe; and

l) the persons responsible for implementing the plan.

Audit reports, with audit results, should be distributed to top management.

Results of the previous audits should be reviewed and the audit programme adjusted to better manage areas experiencing higher risks due to nonconformity.

Other information

Further information can be found in ISO 19011, which provides general guidance on auditing management systems, including the principles of auditing, managing an audit programme and conducting management system audits. It also provides guidance on the evaluation of competence of persons or group of people involved in the audit, including the person managing the audit programme, auditors and audit teams.

Also, in addition to the guidance contained in ISO 19011, further information can be found in:

a) ISO/IEC 27007[1)], which provides specific guidance on managing an ISMS audit programme, on conducting the audits, and on the competence of ISMS auditors; and

b) ISO/IEC 27008[1)], which provides guidance on assessing information security controls.

9.3 Management review

Required activity

Top management reviews the ISMS at planned intervals.

Explanation

The purpose of management review is to ensure the continuing suitability, adequacy and effectiveness of the ISMS. Suitability refers to continuing alignment with the organization's objectives. Adequacy and effectiveness refer to a suitable design and organizational embedding of the ISMS, as well as the effective implementation of processes and controls that are driven by the ISMS.

Overall, management review is a process carried out at various levels in the organization. These activities could vary from daily, weekly, or monthly organizational unit meetings to simple discussions of reports. Top management is ultimately responsible for management review, with inputs from all levels in the organization.

Guidance

Top management should require and regularly review reporting of the performance of the ISMS.

There are many ways in which management can review the ISMS, such as receiving and reviewing measurements and reports, electronic communication, verbal updates. Key inputs are the results of the information security measurements as described in 9.1 and the results of the internal audits described in 9.2 and risk assessment results and risk treatment plan status. When reviewing the results of information security risk assessment and status of the information security risk treatment plan, management should confirm that residual risks meet risk acceptance criteria, and that the risk treatment plan addresses all relevant risks and their risk treatment options.

All aspects of the ISMS should be reviewed by management at planned intervals, at least yearly, by setting up suitable schedules and agenda items in management meetings. New or less mature ISMSs should be reviewed more frequently by management to drive increased effectiveness.

The agenda of the management review should address the following topics:

a) status of actions from previous management reviews;

b) changes in external and internal issues (see 4.1) that are relevant to the ISMS;

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, including suggestions for improvement, requests for change and complaints;

1) Second edition under preparation.

e) results of information security risk assessment(s) and status of information security risk treatment plan; and

f) opportunities for continual improvement, including efficiency improvements of both the ISMS and information security controls.

Inputs to the management review should be at the appropriate level of detail, according to the objectives established for the management involved in the review. For example, top management should evaluate only a summary of all items, according to the information security objectives or high level objectives.

The outputs from the management review process should include decisions related to continual improvement opportunities and any needs for changes to the ISMS. They can also include evidence of decisions regarding:

g) changes of the information security policy and objectives, e.g. driven by changes in external and internal issues and requirements of interested parties;

h) changes of the risk acceptance criteria and the criteria for performing information security risk assessments (see 6.1.2);

i) actions, if needed, following assessment of information security performance;

j) changes of resources or budget for the ISMS;

k) updated information security risk treatment plan or Statement of Applicability; and

l) necessary improvements of monitoring and measurement activities.

Documented information from management reviews is required. It should be retained to demonstrate that consideration has been given to (at least) all the areas listed in ISO/IEC 27001, even where it is decided that no action is necessary.

When several management reviews are done at different levels of the organization, then they should be linked to each other in an appropriate manner.

Other information

No other information.

10 Improvement

10.1 Nonconformity and corrective action

Required activity

The organization reacts to nonconformities, evaluates them and takes corrections as well as corrective actions if needed.

Explanation

A nonconformity is a non-fulfilment of a requirement of the ISMS. Requirements are needs or expectations that are stated, implied or obligatory. There are several types of nonconformities such as:

a) failure to fulfil a requirement (completely or partially) of ISO/IEC 27001 in the ISMS;

b) failure to correctly implement or conform to a requirement, rule or control stated by the ISMS; and

c) partial or total failure to comply with legal, contractual or agreed customer requirements.

Nonconformities can be for example:

d) persons not behaving as expected by procedures and policies;

e) suppliers not providing agreed products or services;

f) projects not delivering expected outcomes; and

g) controls not operating according to design.

Nonconformities can be recognised by:

h) deficiencies of activities performed in the scope of the management system;

i) ineffective controls that are not remediated appropriately;

j) analysis of information security incidents, showing the non-fulfilment of a requirement of the ISMS;

k) complaints from customers;

l) alerts from users or suppliers;

m) monitoring and measurement results not meeting acceptance criteria; and

n) objectives not achieved.

Corrections aim to address the nonconformity immediately and deal with its consequences (ISO/IEC 27001:2013, 10.1 a)).

Corrective actions aim to eliminate the cause of a nonconformity and to prevent recurrence (ISO/IEC 27001:2013, 10.1 b) to g)).

Note that as "as applicable" (ISO/IEC 27001:2013, 10.1 a)) means that if an action to control and correct a nonconformity can be taken, then it needs to be taken.

Guidance

Information security incidents do not necessarily imply that a nonconformity exists, but they can be an indicator of a nonconformity. Internal and external audit and customer complaints are other important sources that help in identifying nonconformities.

The reaction to the nonconformity should be based on a defined handling process. The process should include:

— identifying the extent and impact of the nonconformity;

— deciding on the corrections in order to limit the impact of the nonconformity. Corrections can include switching to previous, failsafe or other appropriate states. Care should be taken that corrections do not make the situation worse;

— communicating with relevant personnel to ensure that corrections are carried out;

— carrying out corrections as decided;

— monitoring the situation to ensure that corrections have had the intended effect and have not produced unintended side-effects;

— acting further to correct the nonconformity if it is still not remediated; and

— communicating with other relevant interested parties, as appropriate.

As an overall result, the handling process should lead to a managed status regarding the nonconformity and the associated consequences. However, corrections alone will not necessarily prevent recurrence of the nonconformity.

Corrective actions can occur after, or in parallel with, corrections. The following process steps should be taken:

1. decide if there is a need to carry out a corrective action, in accordance with established criteria (e.g. impact of the nonconformity, repetitiveness);
2. review of the nonconformity, considering:
   - if similar nonconformities have been recorded;
   - all the consequences and side-effects caused by the nonconformity; and
   - the corrections taken.
3. perform an in-depth cause analysis of the nonconformity, considering:
   - what went wrong, the specific trigger or situation which led to the nonconformity (e.g. mistakes determined by persons, methods, processes or procedures, hardware or software tools, wrong measurements, environment); and
   - patterns and criteria that may help to identify similar situations in the future.
4. perform an analysis of potential consequences on the ISMS, considering:
   - whether similar nonconformities exist in other areas, e.g. by using the patterns and criteria found during the cause analysis; and
   - whether other areas match the identified patterns or criteria, so that it is only a matter of time before a similar nonconformity occurs.
5. determine actions needed to correct the cause, evaluating if they are proportionate to the consequences and impact of the nonconformity, and checking they do not have side-effects which may lead to other nonconformities or significant new information security risks;
6. plan the corrective actions, giving priority, if possible, to areas where there are higher likelihood of recurrence and more significant consequences of the nonconformity. Planning should include a responsible person for a corrective action and a deadline for implementation;
7. implement the corrective actions according to the plan; and
8. assess the corrective actions to determine whether they have actually handled the cause of the nonconformity, and whether it has prevented related nonconformities from occurring. This assessment should be impartial, evidence-based and documented. It should also be communicated to the appropriate roles and interested parties.

As a result of corrections and corrective actions, it is possible that new opportunities for improvement are identified. These should be treated accordingly (see 10.2).

Sufficient documented information is required to be retained to demonstrate that the organization has acted appropriately to address the nonconformity and has dealt with the related consequences. All significant steps of nonconformity management (starting from discovery and corrections) and, if started, corrective action management (cause analysis, review, decision about the implementation of actions, review and change decisions made for the ISMS itself) should be documented. The documented information is also required to include evidence as to whether or not actions taken have achieved the intended effects.

Some organizations maintain registers for tracking nonconformities and corrective actions. There can be more than one register (for example, one for each functional area or process) and on different media (paper, file, application, etc.). If this is the case, then they should be established and controlled as documented information and they should allow a comprehensive review of all nonconformities and corrective actions for ensuring the correct evaluation of the need for actions.

Other information

ISO/IEC 27001 does not explicitly state any requirements for "preventive action". This is because one of the key purposes of a formal management system is to act as a preventive tool. Consequently, the common text used in ISO management system standards requires an assessment of the organization's "external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s)" in 4.1, and to "determine the risks and opportunities that need to be addressed to: assure the ISMS can achieve its intended outcome(s); prevent, or reduce, undesired effects; and achieve continual improvement." in 6.1. These two sets of requirements are considered to cover the concept of "preventive action", and also to take a wider view that looks at risks and opportunities.

10.2 Continual improvement

Required activity

The organization continually improves the suitability, adequacy and effectiveness of the ISMS.

Explanation

Organizations and their contexts are never static. In addition, the risks to information systems, and the ways in which they can be compromised, are evolving rapidly. Finally, no ISMS is perfect; there is always a way in which it can be improved, even if the organization and its context are not changing.

As an example of improvements not linked with nonconformities or risks, the assessment of an element of the ISMS (in terms of suitability, adequacy and effectiveness) can show that it exceeds ISMS requirements or lacks efficiency. If it does, then there can be an opportunity to improve the ISMS by changing the assessed element.

A systematic approach using continual improvement will lead to a more effective ISMS, which will improve the organization's information security. Information security management leads the organization's operational activities in order to avoid being too reactive, i.e. that most of the resources are used for finding problems and addressing these problems. The ISMS is working systematically through continual improvement so that the organization can have a more proactive approach. Top management can set objectives for continual improvement, e.g. through measurements of effectiveness, cost, or process maturity.

As a consequence, the organization treats its ISMS as an evolving, learning, living part of business operations. In order for the ISMS to keep up with changes, it is regularly evaluated with regard to its fitness for purpose, effectiveness, and alignment to the organization's objectives. Nothing is to be taken for granted, and nothing is to be considered as 'off limits' simply because it was good enough at the time it was implemented.

Guidance

Continual improvement of the ISMS should entail that the ISMS itself and all of its elements are assessed considering internal and external issues (4.1), requirements of the interested parties (4.2) and results of performance evaluation (Clause 9). The assessment should include an analysis of:

a) suitability of the ISMS, considering if the external and internal issues, requirements of the interested parties, established information security objectives and identified information security risks are properly addressed through planning and implementation of the ISMS and information security controls;

b) adequacy of the ISMS, considering if the ISMS processes and information security controls are compatible with the organization's overall purposes, activities and processes; and

c) effectiveness of the ISMS, considering if the intended outcome(s) of the ISMS are achieved, the requirements of the interested parties are met, information security risks are managed to meet information security objectives, nonconformities are managed, while resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS are commensurate with those results.

The assessment can also include an analysis of the efficiency of the ISMS and its elements, considering if their use of resources is appropriate, if there is a risk that the lack of efficiency can lead to loss of effectiveness or if there are opportunities for increasing efficiency.

Improvement opportunities can also be identified when managing nonconformities and corrective actions.

Once opportunities for improvement are identified, the organization should, according to 6.1.1:

d) evaluate them to establish whether they are worth pursuing;

e) determine the changes to the ISMS and its elements in order to achieve the improvement;

f) plan and implement the actions to address the opportunities ensuring that benefits are realised, and nonconformities do not occur; and

g) evaluate the effectiveness of the actions.

These actions should be considered as a subset of actions to address risks and opportunities described in 6.1.1.

Other information

No other information.

Annex A
(informative)

Policy framework

Annex A provides guidance on the structure of documentation that includes the information security policy.

In general, a policy is a statement of intentions and direction of an organization as formally expressed by its top management (see ISO/IEC 27000:2016, 2.84).

The content of a policy guides actions and decisions concerning the topic of the policy.

An organization can have a number of policies; one for each of the activity areas that is important to the organization. Some policies are independent of each other, while other policies have a hierarchical relationship.

Typically, an organization has a general policy, e.g. code of conduct, at the highest level of the policy hierarchy. The general policy is supported by other policies addressing different topics and can be applicable to specific areas or functions of the organization. The information security policy is one of these specific policies.

The information security policy is supported by a range of topic-specific policies related to aspects of information security. A number of these are discussed in ISO/IEC 27002, for example the information security policy can be supported by policies concerning access control, information classification (and handling), physical and environmental security, end user oriented topics, amongst others. Additional layers of policies may be added. This arrangement is shown in Figure A.1. Note that some organizations use other terms for topic-specific policy documents, such as “standards”, “directives” or “rules”.

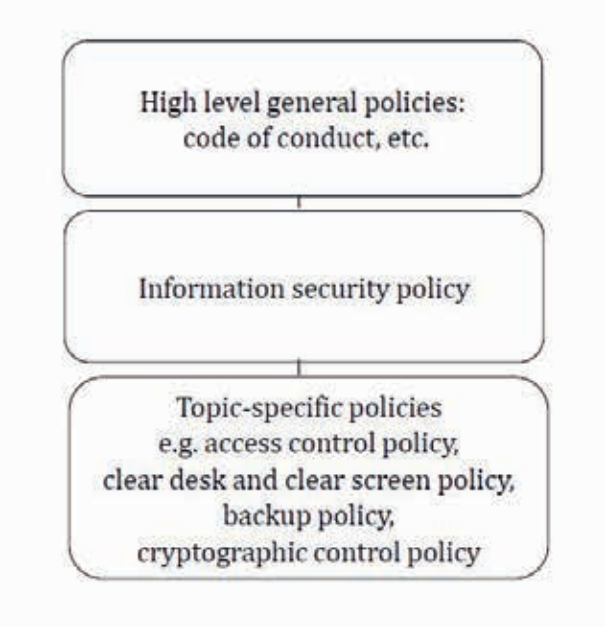

Figure A.1 — Policy hierarchy

ISO/IEC 27001 requires organizations to have an information security policy. It does not, however specify any particular relationship between this policy and other policies of the organization.

The content of policies is based on the context in which an organization operates. Specifically, the following should be considered when developing any policy within the policy framework:

1. the aims and objectives of the organization;
2. strategies adopted to achieve the organization's objectives;
3. the structure and processes adopted by the organization;
4. aims and objectives associated with the topic of the policy;
5. the requirements of related higher level policies; and
6. the target group to be directed by the policy.

This is shown in Figure A.2.

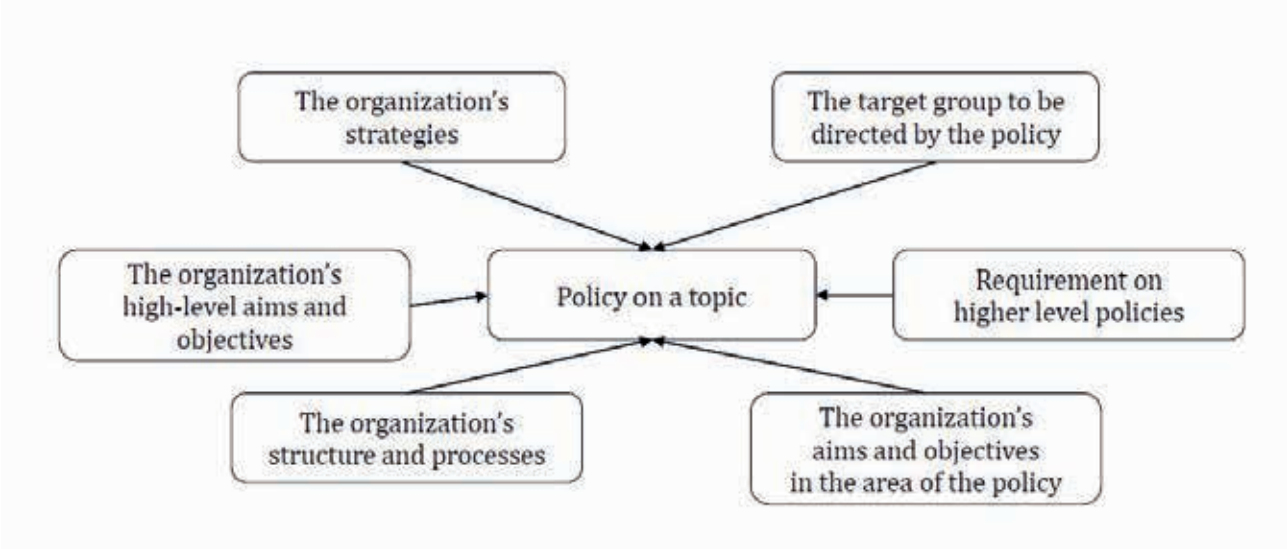

Figure A.2 — Inputs to the development of a policy

Policies can have the following structure:

a) Administrative – policy title, version, publication/validity dates, change history, owner(s) and approver(s), classification, intended audience etc.;

b) Policy summary – a one or two sentence overview. (This can sometimes be merged with the introduction.);

c) Introduction – a brief explanation of the topic of the policy;

d) Scope – describes those parts or activities of an organization that are affected by the policy. If relevant, the scope clause lists other policies that are supported by the policy;

e) Objectives – describes the intent of the policy;

f) Principles – describes the rules concerning actions and decisions for achieving the objectives. In some cases, it can be useful to identify the key processes associated with the topic of the policy and then the rules for operating the processes;

g) Responsibilities – describes who is responsible for actions to meet the requirements of the policy. In some cases, this can include a description of organizational arrangements as well as the responsibilities and authority of persons with designated roles;

h) Key outcomes – describes the business outcomes if the objectives are met. In some cases, this can be merged with the objectives;

i) Related policies – describes other policies relevant to the achievement of the objectives, usually by providing additional detail concerning specific topics; and

j) Policy requirements – describes the detailed requirements of the policy.

Policy content can be organized in a variety of ways. For example, organizations that place emphasis on roles and responsibilities may simplify the description of objectives, and apply the principles specifically to the description of responsibilities.

Bibliography

[1] ISO 19011, *Guidelines for auditing management systems*

[2] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[3] ISO/IEC 27003:2010, *Information technology — Security techniques — Information security management system implementation guidance*

[4] ISO/IEC 27004:2016, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[5] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[6] ISO/IEC 27007[2)], *Information technology — Security techniques — Guidelines for information security management systems auditing*

[7] ISO/IEC/TS 27008[2)], *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[8] ISO 30301, *Information and documentation — Management systems for records — Requirements*

[9] ISO 31000, *Risk management — Principles and guidelines*

2) Under preparation.

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.