INTERNATIONAL STANDARD

ISO/IEC 27001

Redline version compares second edition to first edition

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

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:redline:2014(E)

IMPORTANT — PLEASE NOTE

This is a mark-up copy and uses the following colour coding:

Text example 1	— indicates added text (in green)
~~Text example 2~~	— indicates removed text (in red)
□	— indicates added graphic figure
☒	— indicates removed graphic figure
1.x ...	— Heading numbers containg modifications are highlighted in yellow in the Table of Contents

DISCLAIMER

This Redline version provides you with a quick and easy way to compare the main changes between this edition of the standard and its previous edition. It doesn't capture all single changes such as punctuation but highlights the modifications providing customers with the most valuable information. Therefore it is important to note that this Redline version is not the official ISO standard and that the users must consult with the clean version of the standard, which is the official standard, for implementation purposes.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27001:2005), which has been technically revised.

0 Introduction

~~0.1 General~~

~~This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.~~

~~This International Standard can be used in order to assess conformance by interested internal and external parties.~~

0.1 General

~~0.2 Process approach~~

~~This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.~~

~~An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.~~

~~The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".~~

~~The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:~~

~~a) understanding an organization's information security requirements and the need to establish policy and objectives for information security;~~

~~b) implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;~~

~~c) monitoring and reviewing the performance and effectiveness of the ISMS; and~~

~~d) continual improvement based on objective measurement.~~

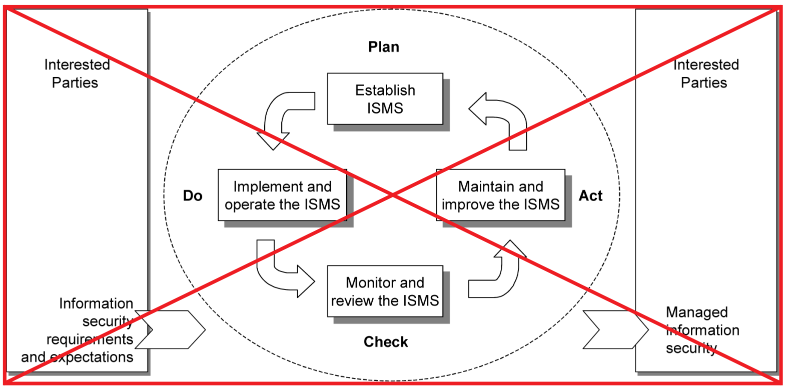
~~This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes. Figure 1 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations. Figure 1 also illustrates the links in the processes presented in Clauses 4, 5, 6, 7 and 8.~~

~~The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002)~~[1] ~~governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.~~

~~EXAMPLE 1 A requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization.~~

[1] ~~OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org~~

~~EXAMPLE 2 An expectation might be that if a serious incident occurs — perhaps hacking of an organization's eBusiness web site — there should be people with sufficient training in appropriate procedures to minimize the impact.~~


Interested Parties
Plan
Establish ISMS
Interested Parties
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Information security requirements and expectations
Managed information security

~~Figure 1 — PDCA model applied to ISMS processes~~

~~**Plan (establish the ISMS)**~~	~~Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.~~
~~**Do (implement and operate the ISMS)**~~	~~Implement and operate the ISMS policy, controls, processes and procedures.~~
~~**Check (monitor and review the ISMS)**~~	~~Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.~~
~~**Act (maintain and improve the ISMS)**~~	~~Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.~~

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

~~0.3 Compatibility with other management systems~~

~~This International Standard is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards. Table C.1 illustrates the relationship between the clauses of this International Standard, ISO 9001:2000 and ISO 14001:2004.~~

~~This International Standard is designed to enable an organization to align or integrate its ISMS with related management system requirements.~~

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

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

~~IMPORTANT —~~ — ~~This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application. Compliance with an International Standard does not in itself confer immunity from legal obligations.~~

1 Scope

~~1.1 General~~

~~This International Standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations). This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.~~

~~The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.~~

~~NOTE 1.~~ ~~References to 'business' in this International Standard should be interpreted broadly to mean those activities that are core to the purposes for the organization's existence.~~

~~NOTE 2.~~ ~~ISO/IEC 17799 provides implementation guidance that can be used when designing controls.~~

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

~~1.2 Application~~

~~The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size and nature. Excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard.~~

~~Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons. Where any controls are excluded, claims of conformity to this International Standard are not acceptable unless such exclusions do not affect the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable legal or regulatory requirements.~~

~~NOTE.~~ ~~If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within this existing management system.~~

2 Normative references

The following ~~referenced documents~~documents, in whole or in part, are normatively referenced in this document and are indispensable for ~~the application of this document~~its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC ~~17799:2005~~27000, *Information technology — Security techniques —* ~~*Code of practice for information security management*~~*Information security management systems — Overview and vocabulary*

3 Terms and definitions

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

~~3~~4 ~~Terms and definitions~~Context of the organization

~~For the purposes of this document, the following terms and definitions apply.~~

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

~~**3.1**~~
~~**asset**~~
~~anything that has value to the organization~~

[SOURCE: ~~ISO/IEC 13335-1:2004~~]

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

~~**3.2**~~
~~**availability**~~
~~the property of being accessible and usable upon demand by an authorized entity~~

[SOURCE: ~~ISO/IEC 13335-1:2004~~]

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2; and

c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

~~**3.3**~~
~~**confidentiality**~~
~~the property that information is not made available or disclosed to unauthorized individuals, entities, or processes~~

[SOURCE: ~~ISO/IEC 13335-1:2004~~]

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

~~**3.4**~~
~~**information security**~~
~~preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved~~

[SOURCE: ~~ISO/IEC 17799:2005~~]

~~**3.5**~~
~~**information security event**~~
~~an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant~~

[SOURCE: ~~ISO/IEC TR 18044:2004~~]

~~**3.6**~~
~~**information security incident**~~
~~a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security~~

[SOURCE: ~~ISO/IEC TR 18044:2004~~]

~~**3.7**~~
~~**information security management system**~~
~~**ISMS**~~
~~that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security~~

~~Note 1 to entry: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.~~

~~**3.8**~~
~~**integrity**~~
~~the property of safeguarding the accuracy and completeness of assets~~

[SOURCE: ~~ISO/IEC 13335-1:2004~~]

~~**3.9**~~
~~**residual risk**~~
~~the risk remaining after risk treatment~~

[SOURCE: ~~ISO/IEC Guide 73:2002~~]

~~**3.10**~~
~~**risk acceptance**~~
~~decision to accept a risk~~

[SOURCE: ~~ISO/IEC Guide 73:2002~~]

~~**3.11**~~
~~**risk analysis**~~
~~systematic use of information to identify sources and to estimate the risk~~

[SOURCE: ~~ISO/IEC Guide 73:2002~~]

~~**3.12**~~
~~**risk assessment**~~
~~overall process of risk analysis and risk evaluation~~

[SOURCE: ~~ISO/IEC Guide 73:2002~~]

~~**3.13**~~
~~**risk evaluation**~~
~~process of comparing the estimated risk against given risk criteria to determine the significance of the risk~~

[SOURCE: ~~ISO/IEC Guide 73:2002~~]

~~**3.14**~~
~~**risk management**~~
~~coordinated activities to direct and control an organization with regard to risk~~

[SOURCE: ~~ISO/IEC Guide 73:2002~~]

~~**3.15**~~
~~**risk treatment**~~
~~process of selection and implementation of measures to modify risk~~

[SOURCE: ~~ISO/IEC Guide 73:2002~~]

~~Note 1 to entry: In this International Standard the term 'control' is used as a synonym for 'measure'.~~

~~**3.16**~~
~~**statement of applicability**~~
~~documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.~~

~~Note 1 to entry: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization's business requirements for information security.~~

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; and

d) includes a commitment to continual improvement of the information security management system.

The information security policy shall:

e) be available as documented information;

f) be communicated within the organization; and

g) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority for:

a) ensuring that the information security management system conforms to the requirements of this International Standard; and

b) reporting on the performance of the information security management system to top management.

NOTE Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

~~4~~6 ~~Information security management system~~Planning

~~4.1 General requirements~~

~~The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organization's overall business activities and the risks it faces. For the purposes of this International Standard the process used is based on the PDCA model shown in Figure 1~~.