INTERNATIONAL STANDARD

ISO/IEC 27001

First edition
2005-10-15

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

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2005(E)

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*.

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.

0.2 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.

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

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.

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.

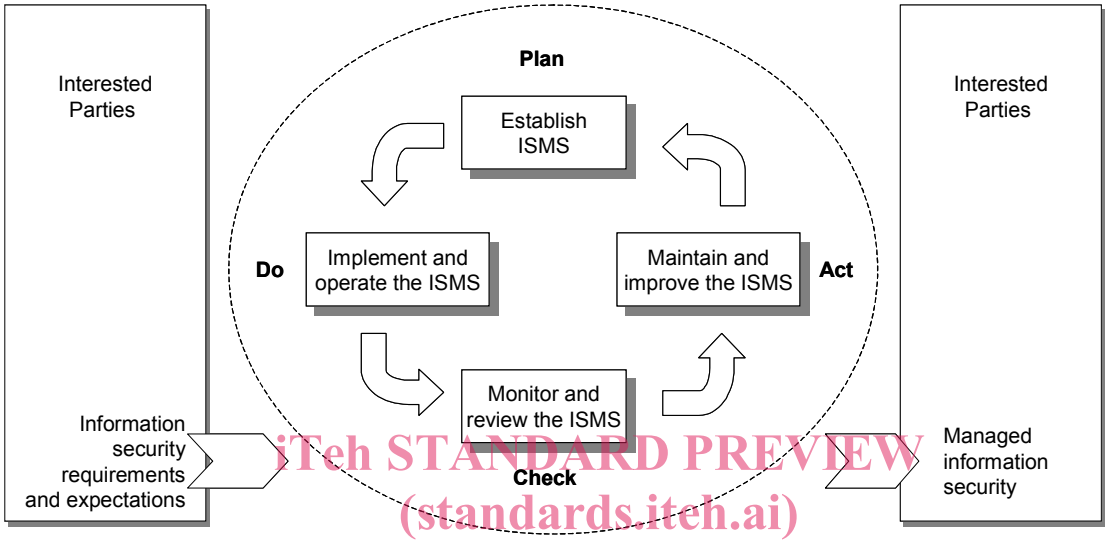

Figure 1 — PDCA model applied to ISMS processes

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.

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.

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.

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 are indispensable for the application 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 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Terms and definitions

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

3.1
asset
anything that has value to the organization

[ISO/IEC 13335-1:2004]

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

[ISO/IEC 13335-1:2004]

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

[ISO/IEC 13335-1:2004]

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

[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

[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

[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: 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

[ISO/IEC 13335-1:2004]

3.9
residual risk
the risk remaining after risk treatment

[ISO/IEC Guide 73:2002]

3.10
risk acceptance
decision to accept a risk

[ISO/IEC Guide 73:2002]

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

[ISO/IEC Guide 73:2002]

3.12
risk assessment
overall process of risk analysis and risk evaluation

[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

[ISO/IEC Guide 73:2002]

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

[ISO/IEC Guide 73:2002]

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

[ISO/IEC Guide 73:2002]

NOTE: 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: 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.

4 Information security management system

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.

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS

The organization shall do the following.

a) Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope (see 1.2).

b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that:

1) includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;

2) takes into account business and legal or regulatory requirements, and contractual security obligations;

3) aligns with the organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place;

4) establishes criteria against which risk will be evaluated (see 4.2.1c)); and

5) has been approved by management.

NOTE: For the purposes of this International Standard, the ISMS policy is considered as a superset of the information security policy. These policies can be described in one document.

c) Define the risk assessment approach of the organization.

1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.

2) Develop criteria for accepting risks and identify the acceptable levels of risk. (see 5.1f)).

The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.

NOTE: There are different methodologies for risk assessment. Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Techniques for the management of IT Security*.

d) Identify the risks.

1) Identify the assets within the scope of the ISMS, and the owners[2)] of these assets.

2) Identify the threats to those assets.

3) Identify the vulnerabilities that might be exploited by the threats.

4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

---

2) The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.

e) Analyse and evaluate the risks.

1) Assess the business impacts upon the organization that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.

2) Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

3) Estimate the levels of risks.

4) Determine whether the risks are acceptable or require treatment using the criteria for accepting risks established in 4.2.1c)2).

f) Identify and evaluate options for the treatment of risks.

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policies and the criteria for accepting risks (see 4.2.1c)2));

3) avoiding risks; and

4) transferring the associated business risks to other parties, e.g. insurers, suppliers.

g) Select control objectives and controls for the treatment of risks.

Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection shall take account of the criteria for accepting risks (see 4.2.1c)2)) as well as legal, regulatory and contractual requirements.

The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover the identified requirements.

The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

NOTE: Annex A contains a comprehensive list of control objectives and controls that have been found to be commonly relevant in organizations. Users of this International Standard are directed to Annex A as a starting point for control selection to ensure that no important control options are overlooked.

h) Obtain management approval of the proposed residual risks.

i) Obtain management authorization to implement and operate the ISMS.

j) Prepare a Statement of Applicability.

A Statement of Applicability shall be prepared that includes the following:

1) the control objectives and controls selected in 4.2.1g) and the reasons for their selection;

2) the control objectives and controls currently implemented (see 4.2.1e)2)); and

3) the exclusion of any control objectives and controls in Annex A and the justification for their exclusion.

NOTE: The Statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.

4.2.2 Implement and operate the ISMS

The organization shall do the following.

a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5).

b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.

c) Implement controls selected in 4.2.1g) to meet the control objectives.

d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3c)).

NOTE: Measuring the effectiveness of controls allows managers and staff to determine how well controls achieve planned control objectives.

e) Implement training and awareness programmes (see 5.2.2).

f) Manage operation of the ISMS.

g) Manage resources for the ISMS (see 5.2).

h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3a)).

4.2.3 Monitor and review the ISMS

The organization shall do the following.

a) Execute monitoring and reviewing procedures and other controls to:

1) promptly detect errors in the results of processing;

2) promptly identify attempted and successful security breaches and incidents;

3) enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected;

4) help detect security events and thereby prevent security incidents by the use of indicators; and

5) determine whether the actions taken to resolve a breach of security were effective.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.

c) Measure the effectiveness of controls to verify that security requirements have been met.

d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks, taking into account changes to:

1) the organization;

2) technology;

3) business objectives and processes;

4) identified threats;

5) effectiveness of the implemented controls; and

6) external events, such as changes to the legal or regulatory environment, changed contractual obligations, and changes in social climate.

e) Conduct internal ISMS audits at planned intervals (see 6).

NOTE: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for internal purposes.

f) Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified (see 7.1).

g) Update security plans to take into account the findings of monitoring and reviewing activities.

h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).

4.2.4 Maintain and improve the ISMS

The organization shall regularly do the following.

a) Implement the identified improvements in the ISMS.

b) Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3. Apply the lessons learnt from the security experiences of other organizations and those of the organization itself.

c) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

d) Ensure that the improvements achieve their intended objectives.

4.3 Documentation requirements

4.3.1 General

Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible.

It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.

The ISMS documentation shall include:

a) documented statements of the ISMS policy (see 4.2.1b)) and objectives;

b) the scope of the ISMS (see 4.2.1a));

c) procedures and controls in support of the ISMS;

d) a description of the risk assessment methodology (see 4.2.1c));

e) the risk assessment report (see 4.2.1c) to 4.2.1g));

f) the risk treatment plan (see 4.2.2b));