INTERNATIONAL STANDARD

ISO/IEC 27000

First edition
2009-05-01

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité des informations — Vue d'ensemble et vocabulaire

Reference number
ISO/IEC 27000:2009(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 27000 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

0 Introduction

0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1 SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards.

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets and prepare for an independent assessment of their ISMS applied to the protection of information, such as financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties.

0.2 ISMS family of standards

The ISMS family of standards[1)] is intended to assist organizations of all types and sizes to implement and operate an ISMS. The ISMS family of standards consists of the following International Standards, under the general title *Information technology — Security techniques*:

— ISO/IEC 27000:2009, *Information security management systems — Overview and vocabulary*

— ISO/IEC 27001:2005, *Information security management systems — Requirements*

— ISO/IEC 27002:2005, *Code of practice for information security management*

— ISO/IEC 27003, *Information security management system implementation guidance*

— ISO/IEC 27004, *Information security management — Measurement*

— ISO/IEC 27005:2008, *Information security risk management*

— ISO/IEC 27006:2007, *Requirements for bodies providing audit and certification of information security management systems*

— ISO/IEC 27007, *Guidelines for information security management systems auditing*

— ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

NOTE The general title "*Information technology — Security techniques*" indicates that these standards were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:

— ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

1) Standards identified throughout this subclause with no release year indicated are still under development.

0.3 Purpose of this International Standard

This International Standard provides an overview of information security management systems, which form the subject of the ISMS family of standards, and defines related terms.

NOTE Annex A provides clarification on how verbal forms are used to express requirements and/or guidance in the ISMS family of standards.

The ISMS family of standards includes standards that:

a) define requirements for an ISMS and for those certifying such systems;

b) provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements;

c) address sector-specific guidelines for ISMS; and

d) address conformity assessment for ISMS.

The terms and definitions provided in this International Standard:

— cover commonly used terms and definitions in the ISMS family of standards;

— will not cover all terms and definitions applied within the ISMS family of standards; and

— do not limit the ISMS family of standards in defining terms for own use.

Standards addressing only the implementation of controls, as opposed to addressing all controls, from ISO/IEC 27002 are excluded from the ISMS family of standards.

To reflect the changing status of the ISMS family of standards, this International Standard is expected to be continually updated on a more frequent basis than would normally be the case for other ISO/IEC standards.

Information technology — Security techniques — Information security management systems — Overview and vocabulary

1 Scope

This International Standard provides:

a) an overview of the ISMS family of standards;

b) an introduction to information security management systems (ISMS);

c) a brief description of the Plan-Do-Check-Act (PDCA) process; and

d) terms and definitions for use in the ISMS family of standards.

This International Standard is applicable to all types of organization (e.g. commercial enterprises, government agencies, non-profit organizations).

2 Terms and definitions

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

NOTE A term in a definition or note which is defined elsewhere in this clause is indicated by boldface followed by its entry number in parentheses. Such a boldface term can be replaced in the definition by its complete definition.

For example:

attack (2.4) is defined as “attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an **asset** (2.3)”;

asset is defined as “anything that has value to the organization”.

If the term “**asset**” is replaced by its definition:

attack then becomes “attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of anything that has value to the organization”.

2.1
access control
means to ensure that access to **assets** (2.3) is authorized and restricted based on business and security requirements

2.2
accountability
responsibility of an entity for its actions and decisions

2.3
asset
anything that has value to the organization

NOTE There are many types of assets, including:

a) **information** (2.18);

b) software, such as a computer program;

c) physical, such as computer;

d) services;

e) people, and their qualifications, skills, and experience; and

f) intangibles, such as reputation and image.

2.4
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an **asset** (2.3)

2.5
authentication
provision of assurance that a claimed characteristic of an entity is correct

2.6
authenticity
property that an entity is what it claims to be

2.7
availability
property of being accessible and usable upon demand by an authorized entity

2.8
business continuity
processes (2.31) and/or **procedures** (2.30) for ensuring continued business operations

2.9
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or **processes** (2.31)

2.10
control
means of managing **risk** (2.34), including **policies** (2.28), **procedures** (2.30), **guidelines** (2.16), practices or organizational structures, which can be administrative, technical, management, or legal in nature

NOTE Control is also used as a synonym for safeguard or countermeasure.

2.11
control objective
statement describing what is to be achieved as a result of implementing **controls** (2.10)

2.12
corrective action
action to eliminate the cause of a detected nonconformity or other undesirable situation

[ISO 9000:2005]

2.13
effectiveness
extent to which planned activities are realized and planned results achieved

[ISO 9000:2005]

2.14
efficiency
relationship between the results achieved and how well the resources have been used

2.15
event
occurrence of a particular set of circumstances

[ISO/IEC Guide 73:2002]

2.16
guideline
recommendation of what is expected to be done to achieve an objective

2.17
impact
adverse change to the level of business objectives achieved

2.18
information asset
knowledge or data that has value to the organization

2.19
information security
preservation of **confidentiality** (2.9), **integrity** (2.25) and **availability** (2.7) of information

NOTE In addition, other properties, such as **authenticity** (2.6), **accountability** (2.2), **non-repudiation** (2.27), and **reliability** (2.33) can also be involved.

2.20
information security event
identified occurrence of a system, service or network state indicating a possible breach of **information security** (2.19) **policy** (2.28) or failure of **controls** (2.10), or a previously unknown situation that may be security relevant

2.21
information security incident
single or a series of unwanted or unexpected **information security events** (2.20) that have a significant probability of compromising business operations and threatening **information security** (2.19)

2.22
information security incident management
processes (2.31) for detecting, reporting, assessing, responding to, dealing with, and learning from **information security incidents** (2.21)

2.23
information security management system
ISMS
part of the overall **management system** (2.26), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve **information security** (2.19)

2.24
information security risk
potential that a **threat** (2.45) will exploit a **vulnerability** (2.46) of an **asset** (2.3) or group of assets and thereby cause harm to the organization

2.25
integrity
property of protecting the accuracy and completeness of **assets** (2.3)

2.26
management system
framework of **policies** (2.28), **procedures** (2.30), **guidelines** (2.16) and associated resources to achieve the objectives of the organization

2.27
non-repudiation
ability to prove the occurrence of a claimed **event** (2.15) or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the **event** (2.15) or action and involvement of entities in the **event** (2.15)

2.28
policy
overall intention and direction as formally expressed by management

2.29
preventive action
action to eliminate the cause of a potential nonconformity or other undesirable potential situation

[ISO 9000:2005]

2.30
procedure
specified way to carry out an activity or a **process** (2.31)

[ISO 9000:2005]

2.31
process
set of interrelated or interacting activities which transforms inputs into outputs

[ISO 9000:2005]

2.32
record
document stating results achieved or providing evidence of activities performed

[ISO 9000:2005]

2.33
reliability
property of consistent intended behaviour and results

2.34
risk
combination of the probability of an **event** (2.15) and its consequence

[ISO/IEC Guide 73:2002]

2.35
risk acceptance
decision to accept a **risk** (2.34)

[ISO/IEC Guide 73:2002]

2.36
risk analysis
systematic use of information to identify sources and to estimate **risk** (2.34)

[ISO/IEC Guide 73:2002]

NOTE Risk analysis provides a basis for **risk evaluation** (2.41), **risk treatment** (2.43) and **risk acceptance** (2.35).

2.37
risk assessment
overall **process** (2.31) of **risk analysis** (2.36) and **risk evaluation** (2.41)

[ISO/IEC Guide 73:2002]

2.38
risk communication
exchange or sharing of information about **risk** (2.34) between the decision-maker and other stakeholders

[ISO/IEC Guide 73:2002]

2.39
risk criteria
terms of reference by which the significance of **risk** (2.34) is assessed

[ISO/IEC Guide 73:2002]

2.40
risk estimation
activity to assign values to the probability and consequences of a **risk** (2.34)

[ISO/IEC Guide 73:2002]

2.41
risk evaluation
process (2.31) of comparing the estimated **risk** (2.34) against given **risk criteria** (2.39) to determine the significance of the **risk** (2.34)

[ISO/IEC Guide 73:2002]

2.42
risk management
coordinated activities to direct and control an organization with regard to **risk** (2.34)

[ISO/IEC Guide 73:2002]

NOTE Risk management generally includes **risk assessment** (2.37), **risk treatment** (2.43), **risk acceptance** (2.35), **risk communication** (2.38), risk monitoring and risk review.

2.43
risk treatment
process (2.31) of selection and implementation of measures to modify **risk** (2.34)

[ISO/IEC Guide 73:2002]