INTERNATIONAL STANDARD

ISO/IEC 27000

Redline version
compares Fifth edition to
Fourth edition

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

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Reference number
ISO/IEC 27000:redline:2018(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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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~~is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. 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~~ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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~~ISO documents 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~~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~~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~~ISO's adherence to the ~~WTO~~World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: ~~Foreword - Supplementary information~~www.iso.org/iso/foreword.html.

~~The committee responsible for this document is~~This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This ~~fourth~~fifth edition cancels and replaces the ~~third~~fourth edition (ISO/IEC 27000:~~2014~~2016), which has been technically revised. The main changes compared to the previous edition are as follows:

— the Introduction has been reworded;

— some terms and definitions have been removed;

— Clause 3 has been aligned on the high-level structure for MSS;

— Clause 5 has been updated to reflect the changes in the standards concerned;

— Annexes A and B have been deleted.

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, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

~~0.2 ISMS family of standards~~

~~The ISMS family of standards (see Clause 4) is intended to assist organizations of all types and sizes to implement and operate an ISMS and consists of the following International Standards, under the general title *Information technology — Security techniques* (given below in numerical order).~~

- ~~ISO/IEC 27000, *Information security management systems — Overview and vocabulary*~~
- ~~ISO/IEC 27001, *Information security management systems — Requirements*~~
- ~~ISO/IEC 27002, *Code of practice for information security controls*~~
- ~~ISO/IEC 27003, *Information security management system implementation guidance*~~
- ~~ISO/IEC 27004, *Information security management — Measurement*~~
- ~~ISO/IEC 27005, *Information security risk management*~~
- ~~ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems*~~
- ~~ISO/IEC 27007, *Guidelines for information security management systems auditing*~~
- ~~ISO/IEC TR 27008, *Guidelines for auditors on information security controls*~~
- ~~ISO/IEC 27009, *Sector-specific application of ISO/IEC 27001 — Requirements*~~
- ~~ISO/IEC 27010, *Information security management for inter-sector and inter-organizational communications*~~
- ~~ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*~~
- ~~ISO/IEC 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*~~
- ~~ISO/IEC 27014, *Governance of information security*~~
- ~~ISO/IEC TR 27015, *Information security management guidelines for financial services*~~
- ~~ISO/IEC TR 27016, *Information security management — Organizational economics*~~
- ~~ISO/IEC 27017, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*~~

— ISO/IEC 27018, *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

— ISO/IEC 27019, *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*

NOTE The general title "*Information technology — Security techniques*" indicates that these International 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, *Health informatics — Information security management in health using ISO/IEC 27002*

0.2 Purpose of this document

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 process to establish, implement, maintain, and improve an ISMS;

c) address sector-specific guidelines for ISMS; and

d) address conformity assessment for ISMS.

0.3 Purpose of this International Standard

This International Standard provides an overview of information security management systems 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 process to establish, implement, maintain, and improve an ISMS;

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;

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

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

0.3 Content of this document

In this document, the following verbal forms are used:

— "shall" indicates a requirement;

— "should" indicates a recommendation;

— “may” indicates a permission;

— “can” indicates a possibility or a capability.

Information marked as “NOTE” is for guidance in understanding or clarifying the associated requirement. “Notes to entry” used in Clause 3 provide additional information that supplements the terminological data and can contain provisions relating to the use of a term.

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

1 Scope

This ~~International Standard~~document provides the overview of information security management systems~~, and~~ (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This ~~International Standard~~document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

The terms and definitions provided in this document

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

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

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

2 Normative references

There are no normative references in this document.

~~2~~3 Terms and definitions

~~For the purposes of this document, the following terms and definitions apply.~~ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

~~2.1~~3.1
access control
means to ensure that access to assets is authorized and restricted based on business and security *requirements* (~~2.63~~3.56)

~~**2.2**~~
~~**analytical model**~~
~~algorithm or calculation combining one or more *base measures* (2.10) and/or *derived measures* (2.22) with associated *decision criteria* (2.21)~~

~~2.3~~3.2
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

~~**2.4**~~
~~**attribute**~~
~~property or characteristic of an *object* (2.55) that can be distinguished quantitatively or qualitatively by human or automated means~~

~~[SOURCE: ISO/IEC 15939:2007, 2.2, modified — "entity" has been replaced by "object" in the definition.]~~

~~2.5~~3.3
audit
systematic, independent and documented *process* (~~2.61~~3.54) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the organization itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

~~2.6~~3.4
audit scope
extent and boundaries of an *audit* (~~2.5~~3.3)

[SOURCE: ISO 19011:2011, 3.14, modified — Note 1 to entry has been deleted.]

~~2.7~~3.5
authentication
provision of assurance that a claimed characteristic of an entity is correct

~~2.8~~3.6
authenticity
property that an entity is what it claims to be

~~2.9~~3.7
availability
property of being accessible and usable ~~upon~~on demand by an authorized entity

~~2.10~~3.8
base measure
measure (~~2.47~~3.42) defined in terms of an ~~*attribute* (2.4)~~attribute and the method for quantifying it

~~[SOURCE: ISO/IEC 15939:2007, 2.3, modified — Note 2 to entry has been deleted.]~~

Note 1 to entry: A base measure is functionally independent of other ~~*measures* (2.47)~~*measures*.

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.3, modified — Note 2 to entry has been deleted.]

~~2.11~~3.9
competence
ability to apply knowledge and skills to achieve intended results

~~2.12~~3.10
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or *processes* (~~2.61~~3.54)

~~2.13~~3.11
conformity
fulfilment of a *requirement* (~~2.63~~3.56)

~~Note 1 to entry: The term "conformance" is synonymous but deprecated.~~

~~2.14~~3.12
consequence
outcome of an *event* (~~2.25~~3.21) affecting *objectives* (~~2.56~~3.49)

~~[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified]~~

Note 1 to entry: An ~~*event* (2.25)~~event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and, in the context of ~~*information security* (2.33)~~ information security, is usually negative.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through knock-on effects.

[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified — Note 2 to entry has been changed after "and".]

~~2.15~~3.13
continual improvement
recurring activity to enhance *performance* (~~2.59~~3.52)

~~2.16~~3.14
control
measure that is modifying *risk* (~~2.68~~3.61)

~~[SOURCE: ISO Guide 73:2009, 3.8.1.1]~~

Note 1 to entry: Controls include any *process* (~~2.61~~3.54), *policy* (~~2.60~~3.53), device, practice, or other actions which modify *risk* (~~2.68~~3.61).

Note 2 to entry: ~~Controls may~~ It is possible that controls not always exert the intended or assumed modifying effect.

[SOURCE: ISO Guide 73:2009, 3.8.1.1 — Note 2 to entry has been changed.]

~~2.17~~3.15
control objective
statement describing what is to be achieved as a result of implementing *controls* (~~2.16~~3.14)

~~2.18~~3.16
correction
action to eliminate a detected *nonconformity* (~~2.53~~3.47)

~~2.19~~3.17
corrective action
action to eliminate the cause of a *nonconformity* (~~2.53~~3.47) and to prevent recurrence

~~**2.20**~~
~~**data**~~
~~collection of values assigned to *base measures* (2.10), *derived measures* (2.22) and/or *indicators* (2.30)~~

~~[SOURCE: ISO/IEC 15939:2007, 2.4, modified — Note 1 to entry has been added.]~~

~~Note 1 to entry: This definition applies only within the context of ISO/IEC 27004.~~

~~**2.21**~~
~~**decision criteria**~~
~~thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result~~

~~[SOURCE: ISO/IEC 15939:2007, 2.7]~~

~~2.22~~3.18
derived measure
measure (~~2.47~~3.42) that is defined as a function of two or more values of *base measures* (~~2.10~~3.8)

[SOURCE: ISO/IEC/IEEE 15939:~~2007, 2.8~~2017, 3.8, modified — Note 1 to entry has been deleted.]

~~2.23~~3.19
documented information
information required to be controlled and maintained by an *organization* (~~2.57~~3.50) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to

— the *management system* (~~2.46~~3.41), including related *processes* (~~2.61~~3.54);

— information created in order for the *organization* (~~2.57~~3.50) to operate (documentation);

— evidence of results achieved (records).

~~2.24~~3.20
effectiveness
extent to which planned activities are realized and planned results achieved

~~2.25~~3.21
event
occurrence or change of a particular set of circumstances

~~[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — Note 4 to entry has been deleted.]~~

Note 1 to entry: An event can be one or more occurrences, and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”.

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — Note 4 to entry has been deleted.]

~~**2.26**~~
~~**executive management**~~
~~person or group of people who have delegated responsibility from the *governing body* (2.29) for implementation of strategies and policies to accomplish the purpose of the *organization* (2.57)~~

~~Note 1 to entry: Executive management is sometimes called *top management* (2.84) and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles.~~

~~2.27~~3.22
external context
external environment in which the organization seeks to achieve its *objectives* (~~2.56~~3.49)

Note 1 to entry: External context can include the following:

— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having impact on the *objectives* of the *organization* (3.50);

— relationships with, and perceptions and values of, external *stakeholders* (3.37).

[SOURCE: ISO Guide 73:2009, 3.3.1.1]

~~Note 2 to entry: External context can include the following:~~

~~— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;~~

~~— key drivers and trends having impact on the *objectives* (2.56) of the *organization* (2.57);~~

~~— relationships with, and perceptions and values of, external *stakeholders* (2.82).~~

