International Standard

Redline version compares Sixth edition to Fifth edition

ISO/IEC 27000

Information security, cybersecurity and privacy protection — Information security management systems — Overview

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Vue d'ensemble

Reference number
ISO/IEC 27000:redline:2026(en)

INFORMATION ON THIS REDLINE VERSION

This document is a **Redline version** published for information purposes. It is intended to assist users in identifying the changes introduced in comparison with the previous edition of the standard.

Additions are highlighted in green. Deletions are indicated by red strikethrough.

For graphics, additions are identified by a green frame, and deletions are indicated by a red cross.

Clause and heading numbers that include modifications are highlighted in yellow in the Table of Contents.

This Redline version is not an official ISO Standard and does not replace the current published edition. Only the current edition of the International Standard is to be regarded as the official document.

Markup used in this Redline version

Text example 1	added text (green highlight)
~~Text example 2~~	deleted text (red strike through)
	added graphics (green frame)
	deleted graphics (red cross)
1.x ...	modified clause and heading numbers (yellow in the Table of Contents)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) ~~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~~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. ~~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 ~~ISO documents~~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 or www.iec.ch/members_experts/refdocs).

~~Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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).~~

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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~~of 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~~www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ~~ISO/IEC JTC 1~~ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, ~~*IT Security techniques*~~*Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This ~~fifth~~sixth edition cancels and replaces the ~~fourth~~fifth edition (ISO/IEC 27000:~~2016~~2018), which has been technically revised. ~~The main changes compared to the previous edition are as follows:~~

The main changes are as follows:

— the ~~Introduction~~title has been ~~reworded~~modified;

~~— some terms and definitions have been removed;~~

— the structure of the document has been changed to stress its primary role, which is to provide an overview of, and explain the relationships between, documents related to ISMS (information security management systems) including ISO/IEC 27001;

— text presenting the concepts and principles of information security and information security management systems has been added;

— Clause 3 has been ~~aligned on the high-level structure for MSS~~modified to only contain definitions for those terms used in presenting the concepts and principles described in this document;

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

~~— Annexes A and B have been deleted.~~

— it is no longer a terminology document.

This document has been given the status of a horizontal document in accordance with the ISO/IEC Directives, Part 1.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

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 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 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.

This document explains the concepts and principles that underpin information security and information security management systems. It provides an overview of all documents related to ISMS (information security management systems) including ISO/IEC 27001 and explains the relationship between them.

Information security, cybersecurity and privacy protection — Information security management systems — Overview

1 Scope

~~This document provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This 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.~~

This document gives an overview of the concepts and principles used in the documents related to information security management systems (ISMS), including ISO/IEC 27001.

This document is considered to be a horizontal document as it provides an explanation of the concepts and principles that underpin information security and ISMS.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain ~~terminological~~terminology 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/

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

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

~~3.3~~
3.1
~~audit~~
information security
~~systematic, independent and documented *process* (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.~~

preservation of *confidentiality* (3.2), *integrity* (3.3) and *availability* (3.4) of information

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

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

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

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

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

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

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

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

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

~~3.10~~
3.2
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or ~~*processes* (3.54)~~ processes

~~3.11~~
3.3
~~**conformity**~~
integrity
~~fulfilment of a *requirement* (3.56)~~

property of accuracy and completeness

3.12
consequence
outcome of an *event* (3.21) affecting *objectives* (3.49)

Note 1 to entry: An 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, 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".]

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

3.14
control
measure that is modifying *risk* (3.61)

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

Note 2 to entry: 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.]

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

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

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

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

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

3.19
3.4
documented information
availability
information required to be controlled and maintained by an *organization* (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* (3.41), including related *processes* (3.54);

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

— evidence of results achieved (records).

property of being accessible and usable on demand by an authorized entity

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

~~**3.21**~~
3.5
event
occurrence or change of a particular set of circumstances

~~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~~ /IEC 27005:2022, 3.1.11, modified — ~~Note 4~~ The two notes to entry ~~has been deleted~~ have been omitted.]

~~**3.22**~~
~~**external context**~~
~~external environment in which the organization seeks to achieve its *objectives* (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]~~

~~**3.23**~~
~~**governance of information security**~~
~~system by which an *organization's* (3.50) *information security* (3.28) activities are directed and controlled~~

~~**3.24**~~
~~**governing body**~~
~~person or group of people who are accountable for the *performance* (3.52) and conformity of the *organization* (3.50)~~

~~Note 1 to entry: The governing body can, in some jurisdictions, be a board of directors.~~

~~**3.25**~~
~~**indicator**~~
~~*measure* (3.42) that provides an estimate or evaluation~~

~~**3.26**~~
~~**information need**~~
~~insight necessary to manage *objectives* (3.49), goals, risks and problems~~

~~[SOURCE: ISO/IEC/IEEE 15939:2017, 3.12]~~

~~**3.27**~~
~~**information processing facilities**~~
~~any information processing system, service or infrastructure, or the physical location housing it~~