INTERNATIONAL STANDARD

ISO/IEC 27000

Fifth edition
2018-02

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 27000:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
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 organizations, governmental and non-governmental, in liaison with ISO, 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 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).

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).

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 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.

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

This fifth edition cancels and replaces the fourth edition (ISO/IEC 27000:2016), 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 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.

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

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.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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/

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
audit
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.

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

3.11
conformity
fulfilment of a *requirement* (3.56)

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
documented information
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).

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

3.21
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, modified — Note 4 to entry has been deleted.]

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

3.28
information security
preservation of *confidentiality* (3.10), *integrity* (3.36) and *availability* (3.7) of information

Note 1 to entry: In addition, other properties, such as *authenticity* (3.6), accountability, *non-repudiation* (3.48), and *reliability* (3.55) can also be involved.

3.29
information security continuity
processes (3.54) and procedures for ensuring continued *information security* (3.28) operations

3.30
information security event
identified occurrence of a system, service or network state indicating a possible breach of *information* security (3.28) *policy* (3.53) or failure of *controls* (3.14), or a previously unknown situation that can be security relevant

3.31
information security incident
single or a series of unwanted or unexpected *information security events* (3.30) that have a significant probability of compromising business operations and threatening *information security* (3.28)

3.32
information security incident management
set of *processes* (3.54) for detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.31)

3.33
information security management system (ISMS) professional
person who establishes, implements, maintains and continuously improves one or more information security management system *processes* (3.54)

3.34
information sharing community
group of *organizations* (3.50) that agree to share information

Note 1 to entry: An organization can be an individual.

3.35
information system
set of applications, services, information technology assets, or other information-handling components

3.36
integrity
property of accuracy and completeness

3.37
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.50) that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.38
internal context
internal environment in which the *organization* (3.50) seeks to achieve its objectives

Note 1 to entry: Internal context can include:

- governance, organizational structure, roles and accountabilities;
- *policies* (3.53), *objectives* (3.49), and the strategies that are in place to achieve them;
- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, *processes* (3.54), systems and technologies);
- *information systems* (3.35), information flows and decision-making *processes* (both formal and informal);
- relationships with, and perceptions and values of, internal *stakeholders* (3.37);
- the organization's culture;
- standards, guidelines and models adopted by the organization;
- form and extent of contractual relationships.

[SOURCE: ISO Guide 73:2009, 3.3.1.2]

3.39
level of risk
magnitude of a *risk* (3.61) expressed in terms of the combination of *consequences* (3.12) and their *likelihood* (3.40)

[SOURCE: ISO Guide 73:2009, 3.6.1.8, modified — “or combination of risks” has been deleted in the definition.]