INTERNATIONAL STANDARD

ISO/IEC 27000

Second edition
2012-12-01

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 27000:2012(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

Foreword

ISO (the International Organisation 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 organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, 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*.

This second edition cancels and replaces the first edition (ISO/IEC 27000:2009).

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, organisations 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[1] (see Clause 4) is intended to assist organisations 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 27000:2009, *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 27003:2010, *Information security management system implementation guidance*

— ISO/IEC 27004:2009, *Information security management — Measurement*

— ISO/IEC 27005:2011, *Information security risk management*

— ISO/IEC 27006:2011, *Requirements for bodies providing audit and certification of information security management systems*

— ISO/IEC 27007:2011, *Guidelines for information security management systems auditing*

— ISO/IEC TR 27008:2011, *Guidelines for auditors on information security management systems controls*

— ISO/IEC 27010:2012, *Information security management guidelines for inter-sector and inter-organisational communications*

— ITU-T X.1051 | ISO/IEC 27011:2008, *Information security management guidelines for telecommunications organisations based on ISO/IEC 27002*

— ISO/IEC FDIS 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

— ITU-T X.1054 | ISO/IEC FDIS 27014, Governance of information security

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

- ISO/IEC TR 27015, *Information security management guidelines for financial services*
- ISO/IEC WD 27016, *Information security management – Organisational economics*

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*

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 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 new terms for use.

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

1 Scope

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

This International Standard is applicable to all types and sizes of organisation (e.g. commercial enterprises, government agencies, not-for-profit organisations).

2 Terms and definitions

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

NOTE 1 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 "any item that has value to the organisation".

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 any item that has value to the organisation".

2.1
access control
means to ensure that access to **assets** (2.4) is authorized and restricted based on business and security requirements

2.2
accountability
assignment of actions and decisions to an entity

2.3
analytical model
algorithm or calculation combining one or more **base** (2.11) and/or **derived measures** (2.21) with associated decision

[ISO/IEC 15939:2007]

2.4
asset
anything that has value to the organisation

NOTE There are many types of assets, including:

a) information;

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.

2.5
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an **asset** (2.4)

2.6
attribute
property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means

[ISO/IEC 15939:2007]

2.7
audit scope
extent and boundaries of an audit

[ISO 9000:2005]

2.8
authentication
provision of assurance that a claimed characteristic of an entity is correct

2.9
authenticity
property that an entity is what it claims to be

2.10
availability
property of being accessible and usable upon demand by an authorized entity

2.11
base measure
measure (2.43) defined in terms of an **attribute** (2.6) and the method for quantifying it

[ISO/IEC 15939:2007]

NOTE A base measure is functionally independent of other measures.

2.12
business continuity
procedures (2.53) and/or **processes** (2.54) for ensuring continued business operations

2.13
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or **processes** (2.54)

2.14
conformity
fulfillment of a requirement

[ISO 9000:2005].

NOTE The term “conformance” is synonymous but deprecated.

2.15
consequence
outcome of an **event** (2.24) affecting objectives

[ISO Guide 73:2009]

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and in the context of information security is usually negative.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

2.16
control
means of managing **risk** (2.61), including **policies** (2.51), **procedures** (2.53), **guidelines** (2.26), practices or organisational structures, which can be of administrative, technical, management, or legal nature

NOTE 1 Controls for information security include any process, policy, procedure, guideline, practice or organisational structure, which can be administrative, technical, management, or legal in nature which modify information security risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

NOTE 3 Control is also used as a synonym for safeguard or countermeasure.

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

2.18
corrective action
action to eliminate the cause of a detected **non-conformity** (2.48) or other undesirable situation

[ISO 9000:2005]

2.19
data
collection of values assigned to **base measures** (2.11), **derived measures** (2.21) and/or **indicators** (2.27)

[ISO/IEC 15939:2007]

NOTE This definition applies only within the context of ISO/IEC 27004:2009.

2.20
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

[ISO/IEC 15939:2007]

2.21
derived measure
measure (2.43) that is defined as a function of two or more values of **base measures** (2.11)

[ISO/IEC 15939:2007]

2.22

effectiveness

extent to which planned activities are realized and planned results achieved

[ISO 9000:2005]

2.23

efficiency

relationship between the results achieved and the resources used

[ISO 9000:2005]

2.24

event

occurrence or change of a particular set of circumstances

[ISO Guide 73:2009]

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

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

2.25

external context

external environment in which the organisation seeks to achieve its objectives

[ISO Guide 73:2009]

NOTE External context can include:

- 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 organisation; and
- relationships with, and perceptions and values of, external stakeholders.

2.26

guideline

description that clarifies what should be done and how, to achieve the objectives set out in **policies** (2.51)

2.27

indicator

measure (2.43) that provides an estimate or evaluation of specified **attributes** (2.6) derived from an **analytical model** (2.3) with respect to defined **information needs** (2.28)

2.28

information need

insight necessary to manage objectives, goals, risks and problems

[ISO/IEC 15939:2007]

2.29

information processing facilities

any information processing system, service or infrastructure, or the physical locations housing them

2.30

information security

preservation of **confidentiality** (2.13), **integrity** (2.36) and **availability** (2.10) of information

NOTE In addition, other properties, such as **authenticity** (2.9), **accountability** (2.2), **non-repudiation** (2.49), and **reliability** (2.56) can also be involved.

2.31
information security event
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

2.32
information security incident
single or a series of unwanted or unexpected **information security events** (2.31) that have a significant probability of compromising business operations and threatening **information security** (2.30)

2.33
information security incident management
processes (2.54) for detecting, reporting, assessing, responding to, dealing with, and learning from **information security incidents** (2.32)

2.34
information security management system
ISMS
part of the overall **management system** (2.42), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve **information security** (2.30)

NOTE The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

2.35
information system
application, service, information technology asset, or any other information handling component

2.36
integrity
property of protecting the accuracy and completeness of **assets** (2.4)

2.37
internal context
internal environment in which the organisation seeks to achieve its objectives

[ISO Guide 73:2009]

NOTE Internal context can include:

- governance, organisational structure, roles and accountabilities;
- policies, objectives, 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, systems and technologies);
- information systems, information flows and decision-making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the organisation's culture;
- standards, guidelines and models adopted by the organisation; and
- form and extent of contractual relationships.

2.38
ISMS project
structured activities undertaken by an organisation to implement an **ISMS** (2.34)

2.39
level of risk
magnitude of a **risk** (2.61) expressed in terms of the combination of **consequences** (2.15) and their **likelihood** (2.40)

[ISO Guide 73:2009]

2.40
likelihood
chance of something happening

[ISO Guide 73:2009]

2.41
management
coordinated activities to direct and control an organisation

[ISO 9000:2005]

2.42
management system
framework of **guidelines** (2.26), **policies** (2.51), **procedures** (2.53), **processes** (2.54) and associated resources aimed at ensuring an organisation meets its objectives

2.43
measure
variable to which a value is assigned as the result of **measurement** (2.44)

[ISO/IEC 15939:2007]

NOTE The term “measures” is used to refer collectively to base measures, derived measures, and indicators.

2.44
measurement
process of obtaining information about the **effectiveness** (2.22) of **ISMS** (2.34) and **controls** (2.16) using a **measurement method** (2.46), a **measurement function** (2.45), an **analytical model** (2.3), and **decision criteria** (2.20)

2.45
measurement function
algorithm or calculation performed to combine two or more **base measures** (2.11)

[ISO/IEC 15939:2007]

2.46
measurement method
logical sequence of operations, described generically, used in quantifying an **attribute** (2.6) with respect to a specified **scale** (2.72)

[ISO/IEC 15939:2007]

NOTE The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished:

- subjective: quantification involving human judgment;
- objective: quantification based on numerical rules.

2.47
measurement results
one or more **indicators** (2.27) and their associated interpretations that address an **information need** (2.28)