DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27000

ISO/IEC JTC **1**/SC **27**	Secretariat: **DIN**
Voting begins on: **2015-03-19**	Voting terminates on: **2015-06-19**

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

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

ICS: 01.040.35; 35.040

Reference number
ISO/IEC DIS 27000:2015(E)

COPYRIGHT PROTECTED DOCUMENT

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) 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. 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. 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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword - Supplementary information

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

This fourth edition cancels and replaces the third edition (ISO/IEC 27000:2014), which has been technically revised.

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 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/DIS 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 PII protection 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 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 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.

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

1 Scope

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

2 Terms and definitions

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

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

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

2.3
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, modified – "entity" has been replaced by "object" in the definition.]

2.5
audit
systematic, independent and documented *process* (2.61) 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: "Audit evidence" and "audit criteria" are defined in ISO 19011.

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

[SOURCE: ISO 19011:2011]

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

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

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

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

[SOURCE: ISO/IEC 15939:2007]

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

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

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

2.13
conformity
fulfilment of a *requirement* (2.63)

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

2.14
consequence
outcome of an *event* (2.25) affecting *objectives* (2.56)

[SOURCE: ISO Guide 73:2009]

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.

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

2.16
control
measure that is modifying *risk* (2.68)

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

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

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

2.19
corrective action
action to eliminate the cause of a *nonconformity* (2.53) 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]

Note 1 to entry: This definition applies only within the context of ISO/IEC 27004:2009.

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]

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

[SOURCE: ISO/IEC 15939:2007]

2.23
documented information
information required to be controlled and maintained by an *organization* (2.57) 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), including related *processes* (2.61);

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

— evidence of results achieved (records).

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

2.25
event
occurrence or change of a particular set of circumstances

[SOURCE: ISO Guide 73:2009]

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".

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 and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles

2.27
external context
external environment in which the organization seeks to achieve its objectives

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: 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* (2.56) of the *organization* (2.57); and

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

2.28
governance of information security
system by which an *organization's* (2.57) information security activities are directed and controlled

2.29
governing body
person or group of people who are accountable for the *performance* (2.59) and conformance of the *organization* (2.57)

Note 1 to entry: Governing body can in some jurisdictions be a board of directors.

2.30
indicator
measure (2.47) that provides an estimate or evaluation of specified *attributes* (2.4) derived from an *analytical model* (2.2) with respect to defined *information needs* (2.31)

2.31
information need
insight necessary to manage objectives, goals, risks and problems

[SOURCE: ISO/IEC 15939:2007]

2.32
information processing facilities
any information processing system, service or infrastructure, or the physical location housing it

2.33
information security
preservation of *confidentiality* (2.12), *integrity* (2.40) and *availability* (2.9) of information

Note 1 to entry: In addition, other properties, such as *authenticity* (2.8), accountability, *non-repudiation* (2.54), and *reliability* (2.62) can also be involved.

2.34
information security continuity
processes (2.61) and procedures for ensuring continued *information security* (2.33) operations

2.35
information security event
identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant

2.36
information security incident
single or a series of unwanted or unexpected *information security events* (2.35) that have a significant probability of compromising business operations and threatening *information security* (2.33)

2.37
information security incident management
processes (2.61) for detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (2.36)

2.38
information sharing community
group of organizations that agree to share information

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

2.39
information system
applications, services, information technology assets, or other information handling components

2.40
integrity
property of accuracy and completeness

2.41
interested party
person or *organization* (2.57) that can affect, be affected by, or perceive themselves to be affected by a decision or activity

2.42
internal context
internal environment in which the organization seeks to achieve its objectives

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: Internal context can include:

— governance, organizational 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 organization's culture;

— standards, guidelines and models adopted by the organization; and

— form and extent of contractual relationships.

2.43
ISMS project
structured activities undertaken by an *organization* (2.57) to implement an ISMS

2.44
level of risk
magnitude of a *risk* (2.68) expressed in terms of the combination of *consequences* (2.14) and their *likelihood* (2.45)

[SOURCE: ISO Guide 73:2009, modified — "or combination of risks," has been deleted.]

2.45
likelihood
chance of something happening

[SOURCE: ISO Guide 73:2009]

2.46
management system
set of interrelated or interacting elements of an *organization* (2.57) to establish *policies* (2.60) and *objectives* (2.56) and *processes* (2.61) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

2.47
measure
variable to which a value is assigned as the result of *measurement* (2.48)

[SOURCE: ISO/IEC 15939:2007]

Note 1 to entry: The term "measures" is used to refer collectively to base measures, derived measures, and indicators.

2.48
measurement
process (2.61) to determine a value

Note 1 to entry: In the context of *information security* (2.33) the process of determining a value requires information about the *effectiveness* (2.24) of an information security *management system* (2.46) and its associated *controls* (2.16) using a *measurement method* (2.50), a *measurement function* (2.49), an *analytical model* (2.2), and *decision criteria* (2.21).

2.49
measurement function
algorithm or calculation performed to combine two or more *base measures* (2.10)

[SOURCE: ISO/IEC 15939:2007]

2.50
measurement method
logical sequence of operations, described generically, used in quantifying an *attribute* (2.4) with respect to a specified *scale* (2.80)

[SOURCE: ISO/IEC 15939:2007]

Note 1 to entry: 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.

