

Redline version
compares third edition
to second 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*

Sample Document

get full document from standards.iteh.ai



Reference number
ISO/IEC 27000:redline:2014(E)

© ISO/IEC 2014

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.



COPYRIGHT PROTECTED DOCUMENT

© ISO 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
0 Introduction	v
1 Scope	1
2 Terms and definitions	1
3 Information security management systems	14
3.1 Introduction	14
3.2 What is an ISMS?	14
3.3 Process approach	16
3.4 Why an ISMS is important	16
3.5 Establishing, monitoring, maintaining and improving an ISMS	18
3.6 ISMS critical success factors	20
3.7 Benefits of the ISMS family of standards	21
4 ISMS family of standards	21
4.1 General information	21
4.2 Standards describing an overview and terminology	24
4.3 Standards specifying requirements	24
4.4 Standards describing general guidelines	25
4.5 Standards describing sector-specific guidelines	27
Annex A (informative) Verbal forms for the expression of provisions	29
Annex B (informative) Term and Term ownership	30
Bibliography	34

get full document from standards.iteh.ai

Foreword

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

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~~third edition cancels and replaces the ~~first~~second edition (ISO/IEC 27000:20092012), which has been technically revised.

Sample Document

get full document from standards.iteh.ai

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~~ 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 standards¹⁾ (see [Clause 4](#)) is intended to assist ~~organisations~~ 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:~~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 controls*
- 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/organizational communications*
- ~~ITU-T X.1051~~ | ISO/IEC 27011:~~2008~~, *Information security management guidelines for telecommunications organisations/organizations 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*
- ISO/IEC TR 27015, *Information security management guidelines for financial services*
- ~~ISO/IEC TR 27016/IEC WD 27016~~, *Information security management — Organisational/Organizational 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*.

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

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:

- define requirements for an ISMS and for those certifying such systems;
- provide direct support, detailed guidance and/or interpretation for the overall ~~Plan-Do-Check-Act (PDCA) processes and requirements~~ process to establish, implement, maintain and improve an ISMS;
- address sector-specific guidelines for ISMS; and
- 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~~ 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.

~~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 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 ~~organisation~~organization (e.g. commercial enterprises, government agencies, not-for-profit ~~organisations~~organizations).

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)~~assets is authorized and restricted based on business and security requirements

~~2.2~~

~~**accountability**~~

~~assignment of actions and decisions to an entity~~

~~2.3~~2.2

analytical model

algorithm or calculation combining one or more *base measures* (~~2.11~~2.10) and/or *derived measures* (~~2.21~~2.22) with associated decision **criteria**

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

2.4

asset

~~anything that has value to the organisation~~

~~Note 1 to entry. 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~~2.3

attack

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

~~2.6~~2.4

attribute

property or characteristic of an ~~object~~ **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.

~~2.7~~2.6

audit scope

extent and boundaries of an ~~audit~~ **audit** (2.5)

[SOURCE: ISO ~~9000:2005~~ 19011:2011]

~~2.8~~2.7

authentication

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

~~2.9~~2.8

authenticity

property that an entity is what it **is** claims to be

~~2.10~~2.9

availability

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

~~2.11~~2.10

base measure

measure (2.43) **2.47** defined in terms of an *attribute* (2.6) **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.

~~2.12~~ **2.11**~~business continuity~~ **competence**

~~procedures (2.53) and/or ability to processes (2.54) for ensuring continued business operations apply~~
knowledge and skills to achieve intended results

~~2.13~~ **2.12****confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or
~~processes (2.54)~~ **processes (2.61)**

~~2.14~~ **2.13****conformity**

~~fulfilment~~ **fulfilment** of a ~~requirement~~ **requirement (2.63)** [ISO 9000:2005]

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

~~2.15~~ **2.14****consequence**

outcome of an ~~event (2.24)~~ **event (2.25)** affecting ~~objectives~~ **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)~~ **performance (2.59)**

2.16**control**

~~means of managing measure that is risk (2.61), including modifying policies (2.51) risk (2.68), procedures (2.53), guidelines (2.26), practices or organisational structures, which can be of administrative, technical, management, or legal nature~~

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: 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~~ **device, practice, or other actions which modify risk.**

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

~~Note 3 to entry: 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**correction**

action to eliminate a detected *nonconformity* (2.53)

~~2.18~~2.19

corrective action

action to eliminate the cause of a ~~detected non-conformity (2.48)~~ **nonconformity (2.53)** or other undesirable situation and to prevent recurrence

~~[SOURCE: ISO 9000:2005]~~

~~2.19~~2.20

data

collection of values assigned to *base measures* (~~2.11~~2.10), *derived measures* (~~2.21~~2.22) and/or *indicators* (~~2.27~~2.30)

[SOURCE: ISO/IEC 15939:2007]

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

~~2.20~~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]

~~2.21~~2.22

derived measure

measure (~~2.43~~2.47) that is defined as a function of two or more values of *base measures* (~~2.11~~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).

~~2.22~~2.24

effectiveness

extent to which planned activities are realized and planned results achieved

~~[SOURCE: ISO 9000:2005]~~

~~2.23~~

~~**efficiency**~~

~~relationship between the results achieved and the resources used~~

~~[SOURCE: ISO 9000:2005]~~

~~2.24~~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

2.25 2.27

external context

external environment in which the ~~organisation~~ *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~~ *objectives* (2.56) of the ~~organisation~~ *organization* (2.57); and
- relationships with, and perceptions and values of, external ~~stakeholders~~ *stakeholders* (2.82).

2.28

governance of information security

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

2.26 2.29

~~guideline~~ governing body

~~description that clarifies what should be done and how, to achieve the objectives~~ person or group of people who are accountable for the *performance* (2.59) ~~set out in~~ and conformance of the ~~policies~~ *organization* (2.57)

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

2.27 2.30

indicator

measure (2.43 2.47) that provides an estimate or evaluation of specified *attributes* (2.6 2.4) derived from an *analytical model* (2.3 2.2) with respect to defined *information needs* (2.28 2.31)

2.28 2.31

information need

insight necessary to manage objectives, goals, risks and problems

[SOURCE: ISO/IEC 15939:2007]

2.29 2.32

information processing facilities

any information processing system, service or infrastructure, or the physical ~~locations housing them~~ *location housing it*

2.30 2.33

information security

preservation of *confidentiality* (2.13 2.12), *integrity* (2.36 2.40) and *availability* (2.10 2.9) of information

Note 1 to entry: In addition, other properties, such as *authenticity* (2.9 2.8), ~~accountability~~ (2.2) *accountability*, *non-repudiation* (2.49 2.54), and *reliability* (2.56 2.62) can also be involved.

2.34

information security continuity

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

~~2.31~~ **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 ~~safeguards~~ **controls**, or a previously unknown situation that may be security relevant

~~2.32~~ **2.36**

information security incident

single or a series of unwanted or unexpected *information security events* (~~2.31~~ **2.35**) that have a significant probability of compromising business operations and threatening *information security* (~~2.30~~ **2.33**)

~~2.33~~ **2.37**

information security incident management

processes (~~2.54~~ **2.61**) for detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (~~2.32~~ **2.36**)

~~2.34~~ **2.38**

~~information security management system~~ **sharing community**

ISMS

~~part of the overall group of organizations that management system (2.42), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve~~ **agree to share information** *information security* (2.30)

Note 1 to entry: ~~The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources~~ **An organization can be an individual.**

~~2.35~~ **2.39**

information system

~~application, service~~ **applications, services**, information technology ~~asset~~ **assets**, or ~~any~~ other information handling ~~component~~ **components**

~~2.36~~ **2.40**

integrity

property of ~~protecting the~~ accuracy and completeness ~~of assets~~ (2.4)

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

~~2.37~~ **2.42**

internal context

internal environment in which the ~~organisation~~ **organization** seeks to achieve its objectives

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: Internal context can include:

- governance, ~~organisational~~ **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;