



BSI Standards Publication

**Information technology
— Security techniques
— Information security
management systems —
Overview and vocabulary
(ISO/IEC 27000:2016)**

National foreword

This British Standard is the UK implementation of EN ISO/IEC 27000:2017. It is identical to ISO/IEC 27000:2016. It supersedes BS ISO/IEC 27000:2016 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee IST/33, IT - Security techniques, to Subcommittee IST/33/-/1, Requirements, security services and guidelines.

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017.
Published by BSI Standards Limited 2017

ISBN 978 0 580 95519 8

ICS 01.040.35; 03.100.70; 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 29 February 2016.

Amendments/corrigenda issued since publication

Date	Text affected
31 March 2017	This corrigendum renumbers BS ISO/IEC 27000:2016 as BS EN ISO/IEC 27000:2017

English Version

Information technology - Security techniques -
Information security management systems - Overview and
vocabulary (ISO/IEC 27000:2016)

Technologies de l'information - Techniques de sécurité
- Systèmes de gestion de sécurité de l'information - Vue
d'ensemble et vocabulaire (ISO/IEC 27000:2016)

Informationstechnik - Sicherheitsverfahren -
Informationssicherheits-Managementsysteme -
Überblick und Terminologie (ISO/IEC 27000:2016)

This European Standard was approved by CEN on 26 January 2017.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of ISO/IEC 27000:2016 has been prepared by Technical Committee ISO/IEC JTC 1 “Information technology” of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27000:2017.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2017, and conflicting national standards shall be withdrawn at the latest by August 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27000:2016 has been approved by CEN as EN ISO/IEC 27000:2017 without any modification.

Contents

Page

Foreword	v
0 Introduction	1
0.1 Overview	1
0.2 ISMS family of standards	1
0.3 Purpose of this International Standard	2
1 Scope	2
2 Terms and definitions	2
3 Information security management systems	14
3.1 General	14
3.2 What is an ISMS?	14
3.2.1 Overview and principles	14
3.2.2 Information	15
3.2.3 Information security	15
3.2.4 Management	15
3.2.5 Management system	16
3.3 Process approach	16
3.4 Why an ISMS is important	16
3.5 Establishing, monitoring, maintaining and improving an ISMS	17
3.5.1 Overview	17
3.5.2 Identifying information security requirements	17
3.5.3 Assessing information security risks	18
3.5.4 Treating information security risks	18
3.5.5 Selecting and implementing controls	18
3.5.6 Monitor, maintain and improve the effectiveness of the ISMS	19
3.5.7 Continual improvement	19
3.6 ISMS critical success factors	20
3.7 Benefits of the ISMS family of standards	20
4 ISMS family of standards	21
4.1 General information	21
4.2 Standards describing an overview and terminology	22
4.2.1 ISO/IEC 27000 (this International Standard)	22
4.3 Standards specifying requirements	22
4.3.1 ISO/IEC 27001	22
4.3.2 ISO/IEC 27006	22
4.4 Standards describing general guidelines	22
4.4.1 ISO/IEC 27002	22
4.4.2 ISO/IEC 27003	23
4.4.3 ISO/IEC 27004	23
4.4.4 ISO/IEC 27005	23
4.4.5 ISO/IEC 27007	23
4.4.6 ISO/IEC TR 27008	23
4.4.7 ISO/IEC 27013	24
4.4.8 ISO/IEC 27014	24
4.4.9 ISO/IEC TR 27016	24
4.5 Standards describing sector-specific guidelines	25
4.5.1 ISO/IEC 27010	25
4.5.2 ISO/IEC 27011	25
4.5.3 ISO/IEC TR 27015	25
4.5.4 ISO/IEC 27017	25
4.5.5 ISO/IEC 27018	26
4.5.6 ISO/IEC TR 27019	26
4.5.7 ISO 27799	26

Annex A (informative) **Verbal forms for the expression of provisions**.....28

Annex B (informative) **Term and term ownership**.....29

Bibliography33

Foreword

ISO (the International 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 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 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).

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. 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 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](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

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

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

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 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 protection of personally identifiable information (PII) 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 International 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, *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.

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* (2.63)

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* (2.21)

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, 2.2, 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, 3.14, modified — Note 1 to entry has been deleted.]

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 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, 2.3, modified — Note 2 to entry has been deleted.]

Note 1 to entry: A base measure is functionally independent of other *measures* (2.47).

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, 3.6.1.3, modified]

Note 1 to entry: An *event* ([2.25](#)) 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* ([2.33](#)) 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, 3.8.1.1]

Note 1 to entry: Controls include any *process* ([2.61](#)), *policy* ([2.60](#)), device, practice, or other actions which modify *risk* ([2.68](#)).

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, 2.4, modified — Note 1 to entry has been added.]

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

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, 2.7]

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, 2.8, modified — Note 1 to entry has been deleted.]

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* (2.57) 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, 3.5.1.3, modified — Note 4 to entry has been deleted.]

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* (2.84) 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* (2.56)

[SOURCE: ISO Guide 73:2009, 3.3.1.1]

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* (2.56) of the *organization* (2.57);

— 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* (2.33) 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* (2.56), goals, risks and problems

[SOURCE: ISO/IEC 15939:2007, 2.12]

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* (2.33) *policy* (2.60) or failure of *controls* (2.16), 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* (2.57) that agree to share information

Note 1 to entry: An *organization* (2.57) can be an individual.