BS EN ISO/IEC 27000:2017

BSI Standards Publication

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

bsi.

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 It supersedes BS ISO/IEC 27000:2016 which is withdrawn.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.

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

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 27000

February 2017

ICS 01.040.35; 03.100.70; 35.030

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

Ref. No. EN ISO/IEC 27000:2017 E

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

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.

INTERNATIONAL STANDARD ISO/IEC 27000:2016(E)

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.

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* (2.57) seeks to achieve its objectives

[SOURCE: ISO Guide 73:2009, 3.3.1.2]

Note 1 to entry: Internal context can include the following:

— governance, organizational structure, roles and accountabilities;

— *policies* (2.60), *objectives* (2.56), 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* (2.61), systems and technologies);

— *information systems* (2.39), information flows and decision-making *processes* (2.61) (both formal and informal);

— relationships with, and perceptions and values of, internal *stakeholders* (2.82);

— the *organization's* (2.57) culture;

— standards, guidelines and models adopted by the *organization* (2.57);

— 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, 3.6.1.8, modified — "or combination of risks" has been deleted in the definition.]

2.45
likelihood
chance of something happening

[SOURCE: ISO Guide 73:2009, 3.6.1.1, modified — Notes 1 and 2 to entry have been deleted.]

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.

Note 3 to entry: The scope of a management system may include the whole of the *organization* (2.57), specific and identified functions of the *organization* (2.57), specific and identified sections of the *organization* (2.57), or one or more functions across a group of *organizations* (2.57).

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

[SOURCE: ISO/IEC 15939:2007, 2.15, modified]

Note 1 to entry: The term "measures" is used to refer collectively to *base measures* (2.10), *derived measures* (2.22), and *indicators* (2.30).

2.48
measurement
process (2.61) to determine a value

Note 1 to entry: In the context of *information security* (2.33), the *process* (2.61) of determining a value requires information about the *effectiveness* (2.24) of an *information security* (2.33) *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, 2.20]

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

Note 1 to entry: The type of measurement method depends on the nature of the operations used to quantify an *attribute* (2.4). Two types can be distinguished as follows:

— subjective: quantification involving human judgment;

— objective: quantification based on numerical rules.

2.51
measurement results
one or more *indicators* (2.30) and their associated interpretations that address an *information need* (2.31)

2.52
monitoring
determining the status of a system, a *process* (2.61) or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

2.53
nonconformity
non-fulfilment of a *requirement* (2.63)

2.54
non-repudiation
ability to prove the occurrence of a claimed *event* (2.25) or action and its originating entities

2.55
object
item characterized through the *measurement* (2.48) of its *attributes* (2.4)

2.56
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (2.61).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an *information security* (2.33) objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of *information security* (2.33) *management systems* (2.46), *information security* (2.33) objectives are set by the organization, consistent with the *information security* (2.33) *policy* (2.60), to achieve specific results.

2.57
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (2.56)

Note 1 to entry: The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

2.58
outsource
make an arrangement where an external *organization* (2.57) performs part of an *organization's* (2.57) function or *process* (2.61)

Note 1 to entry: An external organization is outside the scope of the *management system* (2.46), although the outsourced function or *process* (2.61) is within the scope.

2.59
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (2.61), products (including services), systems or *organizations* (2.57).

2.60
policy
intentions and direction of an *organization* (2.57) as formally expressed by its *top management* (2.84)

2.61
process
set of interrelated or interacting activities which transforms inputs into outputs

2.62
reliability
property of consistent intended behaviour and results

2.63
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (2.57) and interested parties that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (2.23).

2.64
residual risk
risk (2.68) remaining after *risk treatment* (2.79)

Note 1 to entry: Residual risk can contain unidentified *risk* (2.68).

Note 2 to entry: Residual risk can also be known as "retained risk".

2.65
review
activity undertaken to determine the suitability, adequacy and *effectiveness* (2.24) of the subject matter to achieve established *objectives* (2.54)

[SOURCE: ISO Guide 73:2009, 3.8.2.2, modified — Note 1 to entry has been deleted.]

2.66
review object
specific item being reviewed

2.67
review objective
statement describing what is to be achieved as a result of a *review* (2.65)

2.68
risk
effect of uncertainty on objectives

[SOURCE: ISO Guide 73:2009, 1.1, modified]

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an *event* (2.25), its *consequence* (2.14), or *likelihood* (2.45).

Note 3 to entry: Risk is often characterized by reference to potential *events* (2.25) and *consequences* (2.14), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the *consequences* (2.14) of an *event* (2.25) (including changes in circumstances) and the associated *likelihood* (2.45) of occurrence.

Note 5 to entry: In the context of *information security* (2.33) *management systems* (2.46), *information security* (2.33) risks can be expressed as effect of uncertainty on *information security* (2.33) *objectives* (2.56).

Note 6 to entry: *Information security* (2.33) risk is associated with the potential that *threats* (2.83) will exploit *vulnerabilities* (2.89) of an information asset or group of information assets and thereby cause harm to an *organization* (2.57).

2.69
risk acceptance
informed decision to take a particular *risk* (2.68)

[SOURCE: ISO Guide 73:2009, 3.7.1.6]

Note 1 to entry: Risk acceptance can occur without *risk treatment* (2.79) or during the *process* (2.61) of *risk treatment* (2.79).

Note 2 to entry: Accepted *risks* (2.68) are subject to *monitoring* (2.52) and *review* (2.65).

2.70
risk analysis
process (2.61) to comprehend the nature of *risk* (2.68) and to determine the *level of risk* (2.44)

[SOURCE: ISO Guide 73:2009, 3.6.1]

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (2.74) and decisions about *risk treatment* (2.79).

Note 2 to entry: Risk analysis includes risk estimation.

2.71
risk assessment
overall *process* (2.61) of *risk identification* (2.75), *risk analysis* (2.70) and *risk evaluation* (2.74)

[SOURCE: ISO Guide 73:2009, 3.4.1]

2.72
risk communication and consultation
continual and iterative *processes* (2.61) that an organization conducts to provide, share or obtain information, and to engage in dialogue with *stakeholders* (2.82) regarding the management of *risk* (2.68)

Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (2.45), significance, evaluation, acceptability and treatment of *risk* (2.68).

Note 2 to entry: Consultation is a two-way *process* (2.51) of informed communication between an *organization* (2.57) and its *stakeholders* (2.82) on an issue prior to making a decision or determining a direction on that issue. Consultation is

— a *process* (2.61) which impacts on a decision through influence rather than power and

— an input to decision making, not joint decision making.

2.73
risk criteria
terms of reference against which the significance of *risk* (2.68) is evaluated

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

Note 1 to entry: Risk criteria are based on organizational objectives, and *external* (2.27) and *internal context* (2.42).

Note 2 to entry: Risk criteria can be derived from standards, laws, *policies* (2.60) and other *requirements* (2.63).

2.74
risk evaluation
process (2.61) of comparing the results of *risk analysis* (2.70) with *risk criteria* (2.73) to determine whether the *risk* (2.68) and/or its magnitude is acceptable or tolerable

[SOURCE: ISO Guide 73:2009, 3.7.1]

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (2.79).

2.75
risk identification
process (2.61) of finding, recognizing and describing *risks* (2.68)

[SOURCE: ISO Guide 73:2009, 3.5.1]

Note 1 to entry: Risk identification involves the identification of risk sources, *events* (2.25), their causes and their potential *consequences* (2.14).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and *stakeholders'* (2.82) needs.

2.76
risk management
coordinated activities to direct and control an *organization* (2.57) with regard to *risk* (2.68)

[SOURCE: ISO Guide 73:2009, 2.1]

2.77
risk management process
systematic application of management *policies* (2.60), procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing *risk* (2.68)

[SOURCE: ISO Guide 73:2009, 3.1, modified — Note 1 to entry has been added.]

Note 1 to entry: ISO/IEC 27005 uses the term "*process*" (2.61) to describe risk management overall. The elements within the *risk management* (2.76) *process* (2.61) are termed "activities".

2.78
risk owner
person or entity with the accountability and authority to manage a *risk* (2.68)

[SOURCE: ISO Guide 73:2009, 3.5.1.5]

2.79
risk treatment
process (2.61) to modify *risk* (2.68)

[SOURCE: ISO Guide 73:2009, 3.8.1, modified — "decision" has been replaced by "choice" in Note 1 to entry.]

Note 1 to entry: Risk treatment can involve the following:

— avoiding the *risk* (2.68) by deciding not to start or continue with the activity that gives rise to the risk (2.68);

— taking or increasing *risk* (2.68) in order to pursue an opportunity;

— removing the *risk* (2.68) source;

— changing the *likelihood* (2.45);

— changing the *consequences* (2.14);

— sharing the *risk* (2.68) with another party or parties (including contracts and risk financing);

— retaining the *risk* (2.68) by informed choice.

Note 2 to entry: Risk treatments that deal with negative consequences (2.14) are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

Note 3 to entry: Risk treatment can create new *risks* (2.68) or modify existing *risks* (2.68).

2.80
scale
ordered set of values, continuous or discrete, or a set of categories to which the *attribute* (2.4) is mapped

[SOURCE: ISO/IEC 15939:2007, 2.35, modified]

Note 1 to entry: The type of scale depends on the nature of the relationship between values on the scale. Four types of scale are commonly defined as follows:

— nominal: the *measurement* (2.48) values are categorical;

— ordinal: the *measurement* (2.48) values are rankings;

— interval: the *measurement* (2.48) values have equal distances corresponding to equal quantities of the *attribute* (2.4);

— ratio: the *measurement* (2.48) values have equal distances corresponding to equal quantities of the *attribute* (2.4), where the value of zero corresponds to none of the attribute.

These are just examples of the types of scale.

2.81
security implementation standard
document specifying authorized ways for realizing security

2.82
stakeholder
person or *organization* (2.57) that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[SOURCE: ISO Guide 73:2009, 3.2.1.1, modified — Note 1 to entry has been deleted.]

2.83
threat
potential cause of an unwanted incident, which may result in harm to a system or *organization* (2.57)

2.84
top management
person or group of people who directs and controls an *organization* (2.57) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the *organization* (2.57).

Note 2 to entry: If the scope of the *management system* (2.46) covers only part of an *organization* (2.57), then top management refers to those who direct and control that part of the *organization* (2.57).

2.85
trusted information communication entity
autonomous *organization* (2.57) supporting information exchange within an *information sharing community* (2.38)

2.86
unit of measurement
particular quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitude relative to that quantity

[SOURCE: ISO/IEC 15939:2007, 2.40, modified]

2.87
validation
confirmation, through the provision of objective evidence, that the *requirements* (2.63) for a specific intended use or application have been fulfilled

[SOURCE: ISO 9000:2015, 3.8.12, modified]

2.88
verification
confirmation, through the provision of objective evidence, that specified *requirements* (2.63) have been fulfilled

[SOURCE: ISO 9000:2015, 3.8.4]

Note 1 to entry: This could also be called compliance testing.

2.89
vulnerability
weakness of an asset or *control* (2.16) that can be exploited by one or more *threats* (2.83)

3 Information security management systems

3.1 General

Organizations of all types and sizes:

a) collect, process, store, and transmit information;

b) recognize that information, and related processes, systems, networks and people are important assets for achieving organization objectives;

c) face a range of risks that may affect the functioning of assets; and

d) address their perceived risk exposure by implementing information security controls.

All information held and processed by an organization is subject to threats of attack, error, nature (for example, flood or fire), etc., and is subject to vulnerabilities inherent in its use. The term information security is generally based on information being considered as an asset which has a value requiring appropriate protection, for example, against the loss of availability, confidentiality and integrity. Enabling accurate and complete information to be available in a timely manner to those with an authorized need is a catalyst for business efficiency.

Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management.

As information security risks and the effectiveness of controls change depending on shifting circumstances, organizations need to:

a) monitor and evaluate the effectiveness of implemented controls and procedures;

b) identify emerging risks to be treated; and

c) select, implement and improve appropriate controls as needed.

To interrelate and coordinate such information security activities, each organization needs to establish its policy and objectives for information security and achieve those objectives effectively by using a management system.

3.2 What is an ISMS?

3.2.1 Overview and principles

An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information

assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:

a) awareness of the need for information security;

b) assignment of responsibility for information security;

c) incorporating management commitment and the interests of stakeholders;

d) enhancing societal values;

e) risk assessments determining appropriate controls to reach acceptable levels of risk;

f) security incorporated as an essential element of information networks and systems;

g) active prevention and detection of information security incidents;

h) ensuring a comprehensive approach to information security management;

i) continual reassessment of information security and making of modifications as appropriate.

3.2.2 Information

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can be stored in many forms, including: digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information may be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which the information is transmitted, it always needs appropriate protection.

In many organizations, information is dependent upon information and communications technology. This technology is often an essential element in the organization and assists in facilitating the creation, processing, storing, transmitting, protection and destruction of information.

3.2.3 Information security

Information security ensures the confidentiality, availability and integrity of information. Information security involves the application and management of appropriate controls that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing consequences of information security incidents.

Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets. These controls need to be specified, implemented, monitored, reviewed and improved where necessary, to ensure that the specific information security and business objectives of the organization are met. Relevant information security controls are expected to be seamlessly integrated with an organization's business processes.

3.2.4 Management

Management involves activities to direct, control, and continually improve the organization within appropriate structures. Management activities include the act, manner, or practice of organizing, handling, directing, supervising, and controlling resources. Management structures extend from one person in a small organization to management hierarchies consisting of many individuals in large organizations.

In terms of an ISMS, management involves the supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. Management of information security is expressed through the formulation and use of information security policies,

procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

3.2.5 Management system

A management system uses a framework of resources to achieve an organization's objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In terms of information security, a management system allows an organization to:

a) satisfy the information security requirements of customers and other stakeholders;

b) improve an organization's plans and activities;

c) meet the organization's information security objectives;

d) comply with regulations, legislation and industry mandates; and

e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals.

3.3 Process approach

Organizations need to identify and manage many activities in order to function effectively and efficiently. Any activity using resources needs to be managed to enable the transformation of inputs into outputs using a set of interrelated or interacting activities; this is also known as a process. The output from one process can directly form the input to another process and generally this transformation is carried out under planned and controlled conditions. The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

3.4 Why an ISMS is important

Risks associated with an organization's information assets need to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization.

The adoption of an ISMS is expected to be a strategic decision for an organization and it is necessary that this decision is seamlessly integrated, scaled and updated in accordance with the needs of the organization.

The design and implementation of an organization's ISMS is influenced by the needs and objectives of the organization, the security requirements, the business processes employed and the size and structure of the organization. The design and operation of an ISMS needs to reflect the interests and information security requirements of all of the organization's stakeholders including customers, suppliers, business partners, shareholders and other relevant third parties.

In an interconnected world, information and related processes, systems, and networks constitute critical business assets. Organizations and their information systems and networks face security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire and flood. Damage to information systems and networks caused by malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

An ISMS is important to both public and private sector businesses. In any industry, an ISMS is an enabler that supports e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increase the difficulty of controlling access to and handling of information. In addition, the distribution of mobile storage devices containing information assets can weaken the effectiveness of traditional controls. When organizations adopt

the ISMS family of standards, the ability to apply consistent and mutually-recognizable information security principles can be demonstrated to business partners and other interested parties.

Information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the information security that can be achieved through technical means is limited, and may be ineffective without being supported by appropriate management and procedures within the context of an ISMS. Integrating security into a functionally complete information system could be difficult and costly. An ISMS involves identifying which controls are in place and requires careful planning and attention to detail. As an example, access controls, which may be technical (logical), physical, administrative (managerial) or a combination, provide a means to ensure that access to information assets is authorized and restricted based on the business and information security requirements.

The successful adoption of an ISMS is important to protect information assets allowing an organization to:

a) achieve greater assurance that its information assets are adequately protected against threats on a continual basis;

b) maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness;

c) continually improve its control environment; and

d) effectively achieve legal and regulatory compliance.

3.5 Establishing, monitoring, maintaining and improving an ISMS

3.5.1 Overview

An organization needs to undertake the following steps in establishing, monitoring, maintaining and improving its ISMS:

a) identify information assets and their associated information security requirements (see 3.5.2);

b) assess information security risks (see 3.5.3) and treat information security risks (see 3.5.4);

c) select and implement relevant controls to manage unacceptable risks (see 3.5.5);

d) monitor, maintain and improve the effectiveness of controls associated with the organization's information assets (see 3.5.6).

To ensure the ISMS is effectively protecting the organization's information assets on an ongoing basis, it is necessary for steps (a) to (d) to be continually repeated to identify changes in risks or in the organization's strategies or business objectives.

3.5.2 Identifying information security requirements

Within the overall strategy and business objectives of the organization, its size and geographical spread, information security requirements can be identified through an understanding of the following:

a) identified information assets and their value;

b) business needs for information processing, storage and communication;

c) legal, regulatory, and contractual requirements.

Conducting a methodical assessment of the risks associated with the organization's information assets will involve analysing threats to information assets, vulnerabilities to and the likelihood of a threat materializing to information assets, and the potential impact of any information security incident

on information assets. The expenditure on relevant controls is expected to be proportionate to the perceived business impact of the risk materializing.

3.5.3 Assessing information security risks

Managing information security risks requires a suitable risk assessment and risk treatment method which may include an estimation of the costs and benefits, legal requirements, the concerns of stakeholders, and other inputs and variables as appropriate.

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

Risk assessment should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

Risk assessments should be performed periodically to address changes in the information security requirements and in the risk situation, for example in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

The information security risk assessment should have a clearly defined scope in order to be effective and should include relationships with risk assessments in other areas, if appropriate.

ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk reporting, risk monitoring and risk review. Examples of risk assessment methodologies are included as well.

3.5.4 Treating information security risks

Before considering the treatment of a risk, the organization should decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not cost-effective for the organization. Such decisions should be recorded.

For each of the risks identified following the risk assessment, a risk treatment decision needs to be made. Possible options for risk treatment include the following:

a) applying appropriate controls to reduce the risks;

b) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance;

c) avoiding risks by not allowing actions that would cause the risks to occur;

d) sharing the associated risks to other parties, for example insurers or suppliers.

For those risks where the risk treatment decision has been to apply appropriate controls, these controls should be selected and implemented.

3.5.5 Selecting and implementing controls

Once information security requirements have been identified (see 3.5.2), information security risks to the identified information assets have been determined and assessed (see 3.5.3) and decisions for the treatment of information security risks have been made (see 3.5.4), then selection and implementation of controls for risk reduction apply.

Controls should ensure that risks are reduced to an acceptable level taking the following into account:

a) requirements and constraints of national and international legislation and regulations;

b) organizational objectives;

c) operational requirements and constraints;

d) their cost of implementation and operation in relation to the risks being reduced, and remaining proportional to the organization's requirements and constraints;

e) their objectives to monitor, evaluate and improve the efficiency and effectiveness of information security controls to support the organization's aims. The selection and implementation of controls should be documented within a statement of applicability to assist with compliance requirements;

f) the need to balance the investment in implementation and operation of controls against the loss likely to result from information security incidents.

The controls specified in ISO/IEC 27002 are acknowledged as best practices applicable to most organizations and readily tailored to accommodate organizations of various sizes and complexities. Other standards in the ISMS family of standards provide guidance on the selection and application of ISO/IEC 27002 controls for the information security management system.

Information security controls should be considered at the systems and projects requirements specification and design stage. Failure to do so can result in additional costs and less effective solutions, and maybe, in the worst case, inability to achieve adequate security. Controls can be selected from ISO/IEC 27002 or from other control sets, or new controls can be designed to meet the specific needs of the organization. It is necessary to recognize that some controls may not be applicable to every information system or environment, and might not be practicable for all organizations.

Sometimes it takes time to implement a chosen set of controls and during that time the level of risk may be higher than can be tolerated on a long-term basis. Risk criteria should cover tolerability of risks on a short-term basis while controls are being implemented. Interested parties should be informed of the levels of risk that are estimated or anticipated at different points in time as controls are progressively implemented.

It should be kept in mind that no set of controls can achieve complete information security. Additional management actions should be implemented to monitor, evaluate and improve the efficiency and effectiveness of information security controls to support the organization's aims.

The selection and implementation of controls should be documented within a statement of applicability to assist with compliance requirements.

3.5.6 Monitor, maintain and improve the effectiveness of the ISMS

An organization needs to maintain and improve the ISMS through monitoring and assessing performance against organizational policies and objectives, and reporting the results to management for review. This ISMS review will check that the ISMS includes specified controls that are suitable to treat risks within the ISMS scope. Furthermore, based on the records of these monitored areas, it will provide evidence of verification and traceability of corrective, preventive and improvement actions.

3.5.7 Continual improvement

The aim of continual improvement of an ISMS is to increase the probability of achieving objectives concerning the preservation of the confidentiality, availability and integrity of information. The focus of continual improvement is seeking opportunities for improvement and not assuming that existing management activities are good enough or as good as they can.

Actions for improvement include the following:

a) analysing and evaluating the existing situation to identify areas for improvement;

b) establishing the objectives for improvement;

c) searching for possible solutions to achieve the objectives;

d) evaluating these solutions and making a selection;

e) implementing the selected solution;

f) measuring, verifying, analysing and evaluating results of the implementation to determine that the objectives have been met;

g) formalizing changes.

Results are reviewed, as necessary, to determine further opportunities for improvement. In this way, improvement is a continual activity, i.e. actions are repeated frequently. Feedback from customers and other interested parties, audits and review of the information security management system can also be used to identify opportunities for improvement.

3.6 ISMS critical success factors

A large number of factors are critical to the successful implementation of an ISMS to allow an organization to meet its business objectives. Examples of critical success factors include the following:

a) information security policy, objectives, and activities aligned with objectives;

b) an approach and framework for designing, implementing, monitoring, maintaining, and improving information security consistent with the organizational culture;

c) visible support and commitment from all levels of management, especially top management;

d) an understanding of information asset protection requirements achieved through the application of information security risk management (see ISO/IEC 27005);

e) an effective information security awareness, training and education programme, informing all employees and other relevant parties of their information security obligations set forth in the information security policies, standards, etc., and motivating them to act accordingly;

f) an effective information security incident management process;

g) an effective business continuity management approach;

h) a measurement system used to evaluate performance in information security management and feedback suggestions for improvement.

An ISMS increases the likelihood that an organization will consistently achieve the critical success factors required to protect its information assets.

3.7 Benefits of the ISMS family of standards

The benefits of implementing an ISMS will primarily result from a reduction in information security risks (i.e. reducing the probability of, and/or impact caused by, information security incidents). Specifically, benefits realized for an organization to achieve sustainable success from the adoption of the ISMS family of standards include the following:

a) a structured framework supporting the process of specifying, implementing, operating and maintaining a comprehensive, cost-effective, value creating, integrated and aligned ISMS that meets the organization's needs across different operations and sites;

b) assistance for management in consistently managing and operating in a responsible manner their approach towards information security management, within the context of corporate risk management and governance, including educating and training business and system owners on the holistic management of information security;

c) promotion of globally-accepted good information security practices in a non-prescriptive manner, giving organizations the latitude to adopt and improve relevant controls that suit their specific circumstances and to maintain them in the face of internal and external changes;

d) provision of a common language and conceptual basis for information security, making it easier to place confidence in business partners with a compliant ISMS, especially if they require certification against ISO/IEC 27001 by an accredited certification body;

e) increase in stakeholder trust in the organization;

f) satisfying societal needs and expectations;

g) more effective economic management of information security investments.

4 ISMS family of standards

4.1 General information

The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused upon normative standards describing ISMS requirements (ISO/IEC 27001), certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001, and additional requirement framework for sector-specific implementations of the ISMS (ISO/IEC 27009). Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process as well as sector-specific guidance.

Relationships between the ISMS family of standards are illustrated in Figure 1.

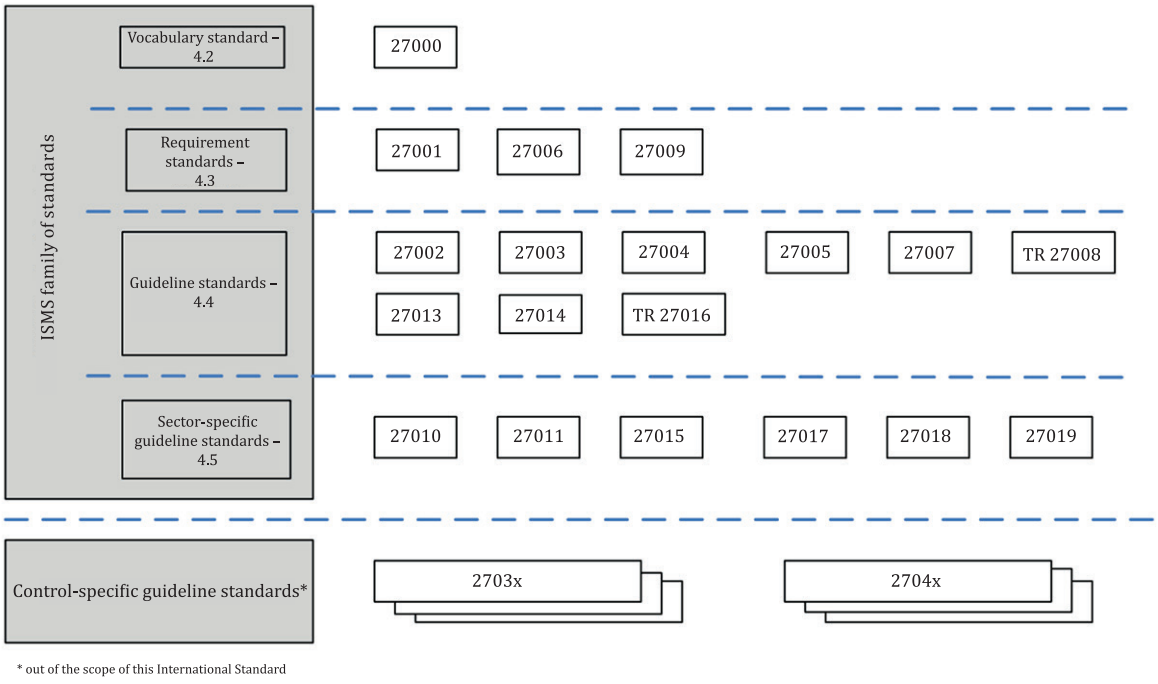

Figure 1 — ISMS family of standards relationships

a) Each of the ISMS family standards is described below by its type (or role) within the ISMS family of standards and its reference number. The applicable clauses are: standards describing an overview and terminology (see 4.2);

b) standards specifying requirements (see 4.3);

c) standards describing general guidelines (see 4.4); or

d) standards describing sector-specific guidelines (see 4.5).

4.2 Standards describing an overview and terminology

4.2.1 ISO/IEC 27000 (this International Standard)

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

Scope: This International Standard provides to organizations and individuals:

a) an overview of the ISMS family of standards;

b) an introduction to information security management systems; and

c) terms and definitions used throughout the ISMS family of standards.

Purpose: This International Standard describes the fundamentals of information security management systems, which form the subject of the ISMS family of standards and defines related terms.

4.3 Standards specifying requirements

4.3.1 ISO/IEC 27001

Information technology — Security techniques — Information security management systems — Requirements

Scope: This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of information security controls customized to the needs of individual organizations or parts thereof. This International Standard can be used by all organizations, regardless of type, size and nature.

Purpose: ISO/IEC 27001 provides normative requirements for the development and operation of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. Organizations operating an ISMS may have its conformity audited and certified. The control objectives and controls from ISO/IEC 27001, Annex A shall be selected as part of this ISMS process as appropriate to cover the identified requirements. The control objectives and controls listed in ISO/IEC 27001, Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002, Clauses 5 to 18.

4.3.2 ISO/IEC 27006

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Scope: This International Standard specifies requirements and provides guidance for bodies providing audit and ISMS certification in accordance with ISO/IEC 27001, in addition to the requirements contained within ISO/IEC 17021. It is primarily intended to support the accreditation of certification bodies providing ISMS certification according to ISO/IEC 27001.

Purpose: ISO/IEC 27006 supplements ISO/IEC 17021 in providing the requirements by which certification organizations are accredited, thus permitting these organizations to provide compliance certifications consistently against the requirements set forth in ISO/IEC 27001.

4.4 Standards describing general guidelines

4.4.1 ISO/IEC 27002

Information technology — Security techniques — Code of practice for information security controls

Scope: This International Standard provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving information security.

Purpose: ISO/IEC 27002 provides guidance on the implementation of information security controls. Specifically, Clauses 5 to 18 provide specific implementation advice and guidance on best practice in support of the controls specified in ISO/IEC 27001, A.5 to A.18.

4.4.2 ISO/IEC 27003

Information technology — Security techniques — Information security management system implementation guidance

Scope: This International Standard provides practical implementation guidance and provides further information for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS in accordance with ISO/IEC 27001.

Purpose: ISO/IEC 27003 provides a process-oriented approach to the successful implementation of the ISMS in accordance with ISO/IEC 27001.

4.4.3 ISO/IEC 27004

Information technology — Security techniques — Information security management — Measurement

Scope: This International Standard provides guidance and advice on the development and use of measurements in order to assess the effectiveness of ISMS, control objectives, and controls used to implement and manage information security, as specified in ISO/IEC 27001.

Purpose: ISO/IEC 27004 provides a measurement framework allowing an assessment of ISMS effectiveness to be measured in accordance with ISO/IEC 27001.

4.4.4 ISO/IEC 27005

Information technology — Security techniques — Information security risk management

Scope: This International Standard provides guidelines for information security risk management. The approach described within this International Standard supports the general concepts specified in ISO/IEC 27001.

Purpose: ISO/IEC 27005 provides guidance on implementing a process-oriented risk management approach to assist in satisfactorily implementing and fulfilling the information security risk management requirements of ISO/IEC 27001.

4.4.5 ISO/IEC 27007

Information technology — Security techniques — Guidelines for information security management systems auditing

Scope: This International Standard provides guidance on conducting ISMS audits, as well as guidance on the competence of information security management system auditors, in addition to the guidance contained in ISO 19011, which is applicable to management systems in general.

Purpose: ISO/IEC 27007 will provide guidance to organizations needing to conduct internal or external audits of an ISMS or to manage an ISMS audit programme against the requirements specified in ISO/IEC 27001.

4.4.6 ISO/IEC TR 27008

Information technology — Security techniques — Guidelines for auditors on information security controls

Scope: This Technical Report provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls, in compliance with an organization's established information security standards.

Purpose: This Technical Report provides a focus on reviews of information security controls, including checking of technical compliance, against an information security implementation standard, which is established by the organization. It does not intend to provide any specific guidance on compliance checking regarding measurement, risk assessment or audit of an ISMS as specified in ISO/IEC 27004, ISO/IEC 27005 or ISO/IEC 27007, respectively. This Technical Report is not intended for management systems audits.

4.4.7 ISO/IEC 27013

Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Scope: This International Standard will provide guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for organizations intending to either:

a) implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented, or vice versa;

b) implement both ISO/IEC 27001 and ISO/IEC 20000-1 together;

c) integrate existing ISO/IEC 27001 and ISO/IEC 20000-1 management systems.

This International Standard focuses exclusively on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1.

Purpose: To provide organizations with a better understanding of the characteristics, similarities and differences of ISO/IEC 27001 and ISO/IEC 20000-1 to assist in the planning of an integrated management system that conforms to both International Standards.

4.4.8 ISO/IEC 27014

Information technology — Security techniques — Governance of information security

Scope: This International Standard will provide guidance on principles and processes for the governance of information security, by which organizations can evaluate, direct and monitor the management of information security.

Purpose: Information security has become a key issue for organizations. Not only are there increasing regulatory requirements but also the failure of an organization's information security measures can have a direct impact on an organization's reputation. Therefore, governing bodies, as part of their governance responsibilities, are increasingly required to have oversight of information security to ensure the objectives of the organization are achieved.

4.4.9 ISO/IEC TR 27016

Information technology — Security techniques — Information security management — Organizational economics

Scope: This Technical Report will provide a methodology allowing organizations to better understand economically how to more accurately value their identified information assets, value the potential risks to those information assets, appreciate the value that information protection controls deliver to these information assets, and determine the optimum level of resources to be applied in securing these information assets.

Purpose: This Technical Report will supplement the ISMS family of standards by overlaying an economics perspective in the protection of an organization's information assets in the context of the

wider societal environment in which an organization operates and providing guidance on how to apply organizational economics of information security through the use of models and examples.

4.5 Standards describing sector-specific guidelines

4.5.1 ISO/IEC 27010

Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

Scope: This International Standard provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities and additionally provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications.

Purpose: This International Standard is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors. In particular, it may be applicable to information exchanges and sharing relating to the provision, maintenance and protection of an organization's or nation state's critical infrastructure.

4.5.2 ISO/IEC 27011

Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Scope: This International Standard provides guidelines supporting the implementation of information security controls in telecommunications organizations.

Purpose: ISO/IEC 27011 allows telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.

4.5.3 ISO/IEC TR 27015

Information technology — Security techniques — Information security management guidelines for financial services

Scope: This Technical Report provides guidelines in addition to the guidance given in the ISO/IEC 27000 family of standards for initiating, implementing, maintaining, and improving information security within organizations providing financial services.

Purpose: This Technical Report is a specialist supplement to ISO/IEC 27001 and ISO/IEC 27002 for use by organizations providing financial services to support them in:

a) initiating, implementing, maintaining, and improving of an information security management system based upon ISO/IEC 27001;

b) designing and implementing controls defined in ISO/IEC 27002 or within this International Standard.

4.5.4 ISO/IEC 27017

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Scope: ISO/IEC 27017 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

— additional implementation guidance for relevant controls specified in ISO/IEC 27002;

— additional controls with implementation guidance that specifically relate to cloud services.

Purpose: This International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

4.5.5 ISO/IEC 27018

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Scope: ISO/IEC 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

Purpose: This International Standard is applicable to organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations. The guidelines in this International Standard may also be relevant to organizations acting as PII controllers; however, PII controllers may be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors, and these are not covered in this International Standard.

4.5.6 ISO/IEC TR 27019

Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Scope: ISO/IEC TR 27019 provides guidelines on information security controls to be implemented in process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes. This includes in particular the following systems, applications and components:

— the overall IT-supported central and distributed process control, monitoring and automation technology as well as IT systems used for their operation, such as programming and parameterization devices;

— digital controllers and automation components such as control and field devices or programmable logic controllers (PLC), including digital sensor and actuator elements;

— all further supporting IT systems used in the process control domain, for example for supplementary data visualization tasks and for controlling, monitoring, data archiving and documentation purposes;

— the overall communications technology used in the process control domain, for example networks, telemetry, telecontrol applications and remote control technology;

— digital metering and measurement devices, for example for measuring energy consumption, generation or emission values;

— digital protection and safety systems, for example protection relays or safety PLCs;

— distributed components of future smart grid environments;

— all software, firmware and applications installed on above mentioned systems.

Purpose: In addition to the security objectives and measures that are set forth in ISO/IEC 27002, this Technical Report provides guidelines for systems used by energy utilities and energy suppliers on information security controls which address further, special requirements.

4.5.7 ISO 27799

Health informatics — Information security management in health using ISO/IEC 27002

Scope: This International Standard provides guidelines supporting the implementation of information security management in health organizations.

Purpose: ISO 27799 provides health organizations with an adaptation of the ISO/IEC 27002 guidelines unique to their industry sector which are additional to the guidance provided towards fulfilling the requirements of ISO/IEC 27001, Annex A.

Annex A
(informative)

Verbal forms for the expression of provisions

Each of the ISMS family of standards documents do not in themselves impose an obligation upon anyone to follow them. However, such an obligation may be imposed, for example, by legislation or by a contract. In order to be able to claim conformity with a document, the user needs to be able to identify the requirements to be satisfied. The user also needs to be able to distinguish these requirements from other recommendations where there is a certain freedom of choice.

The following table clarifies how an ISMS family of standards document is to be interpreted in terms of its verbal expressions as being either requirements or recommendations.

The table is based on the provisions of the ISO/IEC Directives, Part 2:2011, *Rules for the structure and drafting of International Standards,* Annex H.

INDICATION	**EXPLANATION**
Requirement	the terms “shall” and “shall not” indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted
Recommendation	the terms “should” and “should not” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited
Permission	the term “may” and “need not” indicates a course of action permissible within the limits of the document
Possibility	the term “can” and “cannot” indicates a possibility of something occurring

Annex B
(informative)

Term and term ownership

B.1 Term ownership

The **Term Owner** for the ISO/IEC 27000 family of standards is the **standard** that initially defines the term. The **Term Owner** is also responsible for maintaining the definition, i.e.

— providing,

— reviewing,

— updating, and

— removing.

NOTE 1 ISO/IEC 27000 is never determined as the term owner itself.

NOTE 2 ISO/IEC 27001 and ISO/IEC 27006, as normative standards (i.e. containing requirements), always prevail as respective term owner.

B.2 Terms used in these International Standards

B.2.1 ISO/IEC 27001

audit	2.5	measurement	2.48
availability	2.9	monitoring	2.52
competence	2.11	nonconformity	2.53
confidentiality	2.12	objective	2.56
conformity	2.13	organization	2.57
continual improvement	2.15	outsource (verb)	2.58
control	2.16	performance	2.59
correction	2.18	policy	2.60
corrective action	2.19	process	2.61
documented information	2.23	requirement	2.63
effectiveness	2.24	review	2.65
information security	2.33	risk	2.68
integrity	2.40	risk owner	2.78
interested party	2.41	top management	2.84
management system	2.46		

B.2.2 ISO/IEC 27002

access control	2.1	information security event	2.35
attack	2.3	information security incident	2.36
authentication	2.7	information security incident management	2.37
authenticity	2.8	information system	2.39
control objective	2.17	non-repudiation	2.54
information processing facilities	2.32	reliability	2.62
information security continuity	2.34		

B.2.3 ISO/IEC 27003

ISMS project	2.43

B.2.4 ISO/IEC 27004

analytical model	2.2	measurement function	2.49
attribute	2.4	measurement method	2.50
base measure	2.10	measurement results	2.51
data	2.20	object	2.55
decision criteria	2.21	scale	2.80
derived measure	2.22	unit of measurement	2.86
indicator	2.30	validation	2.87
information need	2.31	verification	2.88
measure	2.47		

B.2.5 ISO/IEC 27005

consequence	2.14	risk communication and consultation	2.72
event	2.25	risk criteria	2.73
external context	2.27	risk evaluation	2.74
internal context	2.42	risk identification	2.75
level of risk	2.44	risk management	2.76
likelihood	2.45	risk management process	2.77
residual risk	2.64	risk treatment	2.79
risk acceptance	2.69	threat	2.83
risk analysis	2.70	vulnerability	2.89

risk assessment 2.71

B.2.6 ISO/IEC 27006

certification documents

mark

B.2.7 ISO/IEC 27007

audit scope 2.6

B.2.8 ISO/IEC TR 27008

review object 2.66

review objective 2.67

security implementation standard 2.81

B.2.9 ISO/IEC 27010

information sharing community 2.38

trusted information communication entity 2.85

B.2.10 ISO/IEC 27011

collocation

communication centre

essential communications

non-disclosure of communications

personal information

priority call

telecommunications applications

telecommunications business

telecommunications equipment room

telecommunications facilities

telecommunications organizations

telecommunication records

telecommunications services

telecommunications service customer

telecommunications service user

terminal facilities

user

B.2.11 ISO/IEC 27014

executive management 2.26

governance of information security 2.28

governing body 2.29

stakeholder 2.82

B.2.12 ISO/IEC TR 27015

financial services

B.2.13 ISO/IEC TR 27016

annualized loss expectancy, ALE

loss

direct value
economic comparison
economic factor
economic justification
economic value added
economics
expected value
extended value
indirect value
information security economics
information security management IMS
market value
net present value
non economic benefit
present value
opportunity cost
opportunity value
regulatory requirements
return on investment
societal value
value
value-at-risk

B.2.14 ISO/IEC TR 27017

capability
data breach
secure multi-tenancy
virtual machine

B.2.15 ISO/IEC TR 27018

data breach
personally identifiable information, PII
PII controller
PII principal
PII processor
processing of PII
public cloud service provider

B.2.16 ISO/IEC TR 27019

blackout
Computer Emergency Response Team, CERT
critical infrastructure
debugging
distribution
energy equipment installation
energy supply
energy utility
human-machine interface, HMI
maintenance
PLC
process control system
safety
safety systems
smart grid
statement of applicability, SOA
transmission system

Bibliography

[1] ISO/IEC 17021, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[2] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 19011:2011, *Guidelines for auditing management systems*

[4] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[6] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

[7] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

[8] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[9] ISO/IEC 27006, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[10] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[11] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[12] ISO/IEC 27009, *Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements*

[13] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[14] ISO/IEC 27011, *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[15] ISO/IEC 27013, *Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

[16] ISO/IEC 27014, *Information technology — Security techniques — Governance of information security*

[17] ISO/IEC TR 27015, *Information technology — Security techniques — Information security management guidelines for financial services*

[18] ISO/IEC TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*

[19] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[20] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[20] ISO/IEC 27019, *Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*

[21] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*

[22] ISO Guide 73:2009, *Risk management — Vocabulary*

[23] ISO/IEC 15939:2007, *Systems and software engineering — Measurement process*

[24] ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*

ICS 01.040.35; 35.040

Price based on 34 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.