N1179 Liaison doc JTC1SC27N10001 3rdWD 27000 for comment

Document type: Working draft

Date of document: 2011-06-22

Expected action: COMM

Action due date: 2011-08-28

No. of pages: 41

Background: This JTC 1/SC 27 working draft 'ISO/IEC 3rd WD 27000 (revision) - Information technology - Security techniques - Information security management systems - Overview and vocabulary' submitted for comments. Closing date for SC11 Liaison comments 2011-08-28. Please return your comment to SC 11 Secretariat. ISO Comment template available on SC11 Public document folder.

Committee URL: http://isotc.iso.org/livelink/livelink/open/tc46sc11
ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

<table>
<thead>
<tr>
<th>DOC TYPE:</th>
<th>Working Draft</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE:</td>
<td>Project co-editors (E. Andrukiewicz and R. Kissel)</td>
</tr>
<tr>
<td>DATE:</td>
<td>2011-05-11</td>
</tr>
<tr>
<td>PROJECT:</td>
<td>1.27.52 (27000 revision)</td>
</tr>
<tr>
<td>STATUS:</td>
<td>In accordance with resolution 4 (see SC 27 N10100) of the 42nd SC 27/WG 1 plenary meeting held in Singapore, 11th – 15th April 2011, this document is being circulated for STUDY AND COMMENT. National Bodies and liaison organizations of SC 27 are requested to send their comments / contributions on the above-mentioned Working Draft by 2011-09-12.</td>
</tr>
<tr>
<td>PLEASE NOTE</td>
<td>For comments please use the SC 27 TEMPLATE separately attached to this document.</td>
</tr>
<tr>
<td>ACTION:</td>
<td>COM</td>
</tr>
<tr>
<td>DUE DATE:</td>
<td>2011-09-12</td>
</tr>
<tr>
<td>DISTRIBUTION:</td>
<td>P-, O- and L-Members</td>
</tr>
<tr>
<td></td>
<td>W. Furny, SC 27 Chairman</td>
</tr>
<tr>
<td></td>
<td>M. De Soete, SC 27 Vice Chair</td>
</tr>
<tr>
<td></td>
<td>T. Humphreys, T. Chikazawa, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Convenors</td>
</tr>
<tr>
<td>MEDIUM:</td>
<td><a href="http://isotc.iso.org/livelink/livelink/open/jtc1sc27">http://isotc.iso.org/livelink/livelink/open/jtc1sc27</a></td>
</tr>
<tr>
<td>NO. OF PAGES:</td>
<td>1 + 40</td>
</tr>
</tbody>
</table>
Information technology – Security techniques – Information security management systems – Overview and vocabulary

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information —
Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat of ISO/IEC JTC 1/SC 27
DIN German Institute for Standardization
DE-10772 Berlin

Tel. + 49 30 2601 2652
Fax + 49 30 2601 4 2652
E-mail krystyna.passia@din.de
Web http://www.jtc1sc27.din.de/en (public web site)
http://isotc.iso.org/livelink/livelink/open/jtc1sc27 (SC 27 documents)

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.
Contents

Editors' Notes – History of the Revision ........................................................................................................................................... vi
Foreword .................................................................................................................................................................................................. vii

0 Introduction ............................................................................................................................................................................................................................................. viii
  0.1 Overview ........................................................................................................................................................................................................................................... viii
  0.2 ISMS family of standards .............................................................................................................................................................................................................. viii
  0.3 Purpose of this International Standard ................................................................................................................................................................. ix

1 Scope ...................................................................................................................................................................................................................................................... 1

2 Terms and definitions ......................................................................................................................................................................................................................... 1

3 Information security management systems ................................................................................................................................................................. 13
  3.1 Introduction ........................................................................................................................................................................................................................................... 13
  3.2 What is an ISMS? .............................................................................................................................................................................................................................. 14
    3.2.1 Overview and principles .................................................................................................................................................................................................. 14
    3.2.2 Information ......................................................................................................................................................................................................................... 14
    3.2.3 Information security .................................................................................................................................................................................................. 15
    3.2.4 Management ...................................................................................................................................................................................................................... 15
    3.2.5 Management system ......................................................................................................................................................................................................... 15
  3.3 Process approach .............................................................................................................................................................................................................. 16
  3.4 Why an ISMS is important ............................................................................................................................................................................................................. 16
  3.5 Establishing, monitoring, maintaining and improving an ISMS ........................................................................................................................................................................... 18
    3.5.1 Overview .............................................................................................................................................................................................................................. 18
    3.5.2 Identifying information security requirements ........................................................................................................................................................................ 18
    3.5.3 Assessing information security risks ................................................................................................................................................................................. 18
    3.5.4 Treating information security risks ..................................................................................................................................................................................... 19
    3.5.5 Selecting and implementing controls ................................................................................................................................................................................. 19
    3.5.6 Monitor, maintain and improve the effectiveness of the ISMS ..................................................................................................................................................... 20
  3.6 ISMS critical success factors ............................................................................................................................................................................................................. 20
  3.7 Benefits of the ISMS family of standards ............................................................................................................................................................................. 21

4 ISMS family of standards ................................................................................................................................................................................................................................. 21
  4.1 General information .............................................................................................................................................................................................................. 21
  4.2 Standards describing an overview and terminology ........................................................................................................................................................................... 23
    4.2.1 ISO/IEC 27000 (this document) ......................................................................................................................................................................................... 23
  4.3 Standards specifying requirements ................................................................................................................................................................................................ 23
    4.3.1 ISO/IEC 27001 ......................................................................................................................................................................................................................... 23
    4.3.2 ISO/IEC 27006 ......................................................................................................................................................................................................................... 24
  4.4 Standards describing general guidelines ...................................................................................................................................................................................... 24
    4.4.1 ISO/IEC 27002 ......................................................................................................................................................................................................................... 24
    4.4.2 ISO/IEC 27003 ......................................................................................................................................................................................................................... 24
    4.4.3 ISO/IEC 27004 ......................................................................................................................................................................................................................... 24
    4.4.4 ISO/IEC 27005 ......................................................................................................................................................................................................................... 25
    4.4.5 ISO/IEC 27007 ......................................................................................................................................................................................................................... 25
    4.4.6 ISO/IEC 27008 ......................................................................................................................................................................................................................... 25
    4.4.7 ISO/IEC 27013 ......................................................................................................................................................................................................................... 25
    4.4.8 ISO/IEC 27014 ......................................................................................................................................................................................................................... 26
4.4.9 ISO/IEC TR 27016 ........................................................................................................26
4.5 Standards describing sector-specific guidelines ...................................................26
  4.5.1 ISO/IEC 27010 ....................................................................................................26
  4.5.2 ISO/IEC 27011 ..................................................................................................27
  4.5.3 ISO/IEC 27015 ..................................................................................................27
  4.5.4 ISO 27799 .........................................................................................................27

Annex A (informative) Verbal forms for the expression of provisions .................29

Bibliography ...............................................................................................................30
Editors’ Notes – History of the Revision

The following notes are summarizing the results achieved and open issues identified during last meetings when discussing the revision of ISO/IEC 27000.

1. Decisions taken

A. Terms and Definitions – keeping track of changes
At the meeting in Berlin (10’10), it was decided to create a separate document (WG1 Vocabulary Editing Document) where all changes proposed for the vocabulary of all WG1 family of standards are to be recorded. All Project Editors are instructed to transfer to 27000 Project Editors all changes they recognize in the context of the respective project. WG1 Editing Vocabulary Document is maintained by 27000 Project Editors and updated after every WG1 meeting.

B. Terms and Definitions – Term Owners
For every Term the Owner has been identified: Editor(s) of the project impacted (see sc27n9473 Annex A). Term Owners are responsible for assessing potential impact of the change on their Projects and give a feedback to 27000 Project Editors.

Project Editors draw the NBs attention to this document as it keeps all changes to the vocabulary, and any action to the Clause 3 (Terms and Definitions) of ISO/IEC 27000, and shall reflect current status of an appropriate term and its Term Owner.

C. Strategy and Plan for the Revision
At the meeting in Singapore (04’11), the strategy for the revision has been decided (see the figure below).

Source: SC27N9690 – comment JP 02

In consequence, the plan is to prepare 1st Revision of ISO/IEC 27000:2009 to encompass all changes related to published standards of the 27000 family after the date of ISO/IEC 27000 publication, or those for which publication is expected before ISO/IEC 27000 (Edition 2) reaches the DIS/FDIS stage. Subsequent 2nd Revision of ISO/IEC 27000 will be continued upon completion of the 27001/27002 revision process.
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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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

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

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

0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1 SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards.

Through the use of the ISMS family of standards, 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 1) 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:

— ISO/IEC 27000:2009, Information security management systems — Overview and vocabulary

— ISO/IEC 27001:2005, Information security management systems — Requirements


— ISO/IEC 27003:2010, Information security management system implementation guidance


— ISO/IEC FDIS 27005 (Ed 2), Information security risk management

1) Standards identified throughout this subclause with no release year indicated are still under development.
03 Purpose of this International Standard

This International Standard provides an overview of information security management systems, and defines related terms.

NOTE Annex A provides clarification on how verbal forms are used to express requirements and/or guidance in the ISMS family of standards.

The ISMS family of standards includes standards that:

a) define requirements for an ISMS and for those certifying such systems;

b) provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA)

c) address sector-specific guidelines for ISMS; and

d) address conformity assessment for ISMS.

The terms and definitions provided in this International Standard:
cover commonly used terms and definitions in the ISMS family of standards;

will not cover all terms and definitions applied within the ISMS family of standards; and

do not limit the ISMS family of standards in defining new terms for use.
1 Information technology — Security techniques — Information security management systems — Overview and vocabulary

1 Scope

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 and definitions.

This International Standard is applicable to all types of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

Editors’ note: Following the decision taken at the meeting in Berlin the scope will be extended to contain control-specific part of the ISMS family of standards as well (numbered 27031-40); therefore NB are kindly asked to provide the input for the scope; however, this decision should be reconsidered having in mind the strategy for ISO/IEC 27000- Revision process (see Editor’s Notes History of the Revision, Decision no. 1C)

2 Terms and definitions

For the purposes of the ISMS family of standards, the following terms and definitions apply.

NOTE 1 A term in a definition or note which is defined elsewhere in this clause is indicated by boldface followed by its entry number in parentheses. Such a boldface term can be replaced in the definition by its complete definition.

For example:

attack (2.4) is defined as "attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (2.3);"

asset is defined as "any item that has a distinct value to the organization".

If the term “asset” is replaced by its definition:

attack then becomes "attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of any item that has a distinct value to the organization".

Editors’ note: As a consequence of the decision no. 1C (see Editor’s Notes - History of the Revision), following changes to the definition clause have been made:

- definitions from ISMS standards not being included in ISO/IEC 27000:2009 (ie. 27003, 27004 and 27008) have been added
- definitions from ISO/IEC FDIS 27005 have been updated or reverted
- definitions from ISO/IEC 27001:2005 and 27002:2005 have been reverted to their original contents, if necessary (all subsequent changes as resulted from revision processes of 27001 and 27002 have been recorded for future work, but temporarily skipped for 27000 (Ed 2))

All decisions related to the set of definitions are recorded in SC27N9878.

2.1 access control

means to ensure that access to assets (2.4) is authorized and restricted based on business and security requirements
2.2 accountability
assignment of actions and decisions to an entity

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

[ISO/IEC 15939:2007]

2.4 asset
anything that has value to the organization

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

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

[ISO/IEC 15939:2007]

2.7 audit scope
extent and boundaries of an audit

[ISO 19011:201x]

Editors' Note: Fixed date of will be added as soon as ISO 19011 is published

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

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

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

2.11 base measure
measure (2.45) defined in terms of an attribute (2.6) and the method for quantifying it

[ISO/IEC 15939:2007]
NOTE A base measure is functionally independent of other measures.

2.12 business continuity procedures (2.54) and/or processes (2.55) for ensuring continued business operations

2.13 confidentiality property that information is not made available or disclosed to unauthorized individuals, entities, or processes (2.55)

2.14 conformity fulfillment of a requirement

NOTE: The term “conformance” is synonymous but deprecated.

2.15 consequence outcome of an event (2.24) affecting objectives


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

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

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

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

2.16 control means of managing risk (2.62), including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature

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

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

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

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

2.18 corrective action action to eliminate the cause of a detected non-conformity (2.49) or other undesirable situation
2.19 data
collection of values assigned to base measures (2.11), derived measures (2.21) and/or indicators (2.27)

2.20 decision criteria
thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result

2.21 derived measure
measure (2.44) that is defined as a function of two or more values of base measures (2.11)

2.22 effectiveness
relationship between the result achieved and the resources used [ISO 9000:2005]

2.23 efficiency
relationship between the results achieved and the resources used

2.24 event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.
NOTE 2 An event can consist of something not happening.
NOTE 3 An event can sometimes be referred to as an "incident" or "accident".

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

NOTE External context can include:
— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
— key drivers and trends having impact on the objectives of the organization; and
— relationships with, and perceptions and values of, external stakeholders.

2.26 guideline
description that clarifies what should be done and how, to achieve the objectives set out in policies (2.52)

2.27 indicator
measure (2.44) that provides an estimate or evaluation of specified attributes (2.6) derived from an analytical model (2.3) with respect to defined information needs (2.28)

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

[ISO/IEC 15939:2007]

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

2.30 information security
preservation of confidentiality (2.13), integrity (2.37) and availability (2.10) of information

NOTE In addition, other properties, such as authenticity (2.9), accountability (2.2), non-repudiation (2.50), and reliability (2.57) can also be involved.

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

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

2.33 information security incident management
processes (2.55) for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (2.32)
2.34 information security management
a business risk-based approach, to establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security (2.30)

2.35 information security management system
ISMS
part of the overall management system (2.43), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (2.30)

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

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

Editors’ Note: There is a recommendation from 27000 editing group to change this definition to:
"system which consists of applications, services, information technology assets or other information handling components" (see N9878, Clause 7.6). NBs are asked to consider this proposal.

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

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


NOTE Internal context can include:

— governance, organizational structure, roles and accountabilities;
— policies, objectives, and the strategies that are in place to achieve them;
— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
— information systems, information flows and decision-making processes (both formal and informal);
— relationships with, and perceptions and values of, internal stakeholders;
— the organization's culture;
— standards, guidelines and models adopted by the organization; and
— form and extent of contractual relationships.

2.39 ISMS project
structured activities undertaken by an organization to implement an ISMS (2.34)
2.40 **level of risk**
magnitude of a **risk** (2.62) expressed in terms of the combination of **consequences** (2.15) and their **likelihood** (2.41)


2.41 **likelihood**
chance of something happening


2.42 **management**
coordinated activities to direct and control an organization

2.43 **management system**
framework of **guidelines** (2.26), **policies** (2.52), **procedures** (2.54) and **processes** (2.) associated resources aimed at ensuring an organization meets its objectives

2.44 **measure**
variable to which a value is assigned as the result of **measurement** (2.45)

[ISO/IEC 15939:2007]

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

2.45 **measurement**
process of obtaining information about the **effectiveness** (2.22) of **ISMS** (2.35) and **controls** (2.16) using a **measurement method** (2.47), a **measurement function** (2.46), an **analytical model** (2.3), and **decision criteria** (2.20)

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

[ISO/IEC 15939:2007]

2.47 **measurement method**
logical sequence of operations, described generically, used in quantifying an **attribute** (2.6) with respect to a specified **scale** (2.73)

[ISO/IEC 15939:2007]

NOTE The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished:
subjective: quantification involving human judgment;
objective: quantification based on numerical rules.

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

2.49 non-conformity
non-fulfilment of a requirement

[ISO 9000:2005]

2.50 non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

2.51 object
item characterized through the measurement (2.45) of its attributes (2.6)

2.52 policy
overall intention and direction as formally expressed by management

2.53 preventive action
action to eliminate the cause of a potential nonconformity (2.49) or other undesirable
potential situation

[ISO 9000:2005]

2.54 procedure
specified way to carry out an activity or a process (2.55)

[ISO 9000:2005]

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

[ISO 9000:2005]

2.56 record
document stating results achieved or providing evidence of activities performed

[ISO 9000:2005]
2.57 reliability
property of consistent intended behaviour and results

2.58 residual risk
risk (2.62) remaining after risk treatment (2.72)

NOTE 1 Residual risk can contain unidentified risk.
NOTE 2 Residual risk can also be known as “retained risk”.

2.59 review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

2.60 review object
specific item being reviewed

2.61 review objective
statement describing what is to be achieved as a result of a review

2.62 risk
effect of uncertainty on objectives


NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, information security, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential events (3.3) and consequences (3.1), or a combination of these.

NOTE 4 Information security risk is often expressed in terms of a combination of the consequences of an information security event and the associated likelihood (3.9) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 6 Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

2.63 risk acceptance
decision to accept a risk (2.62)[ISO Guide 73:2002]
2.64 **risk analysis**
process to comprehend the nature of risk (2.62) and to determine the level of risk (2.40)


NOTE 1 Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2 Risk analysis includes risk estimation

2.65 **risk assessment**
overall process (2.55) of risk identification (2.69), risk analysis (2.64) and risk evaluation (2.68)


2.66 **risk communication and consultation**
continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders (2.75) regarding the management of risk (2.62)


NOTE 1 The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

- a process which impacts on a decision through influence rather than power; and
- an input to decision making, not joint decision making.

2.67 **risk criteria**
terms of reference against which the significance of risk (2.45) is evaluated


NOTE 1 Risk criteria are based on organizational objectives, and external and internal context.

NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements

2.68 **risk evaluation**
process (2.55) of comparing the results of risk analysis (2.64) with risk criteria (2.67) to determine whether the risk (2.62) and/or its magnitude is acceptable or tolerable


NOTE Risk evaluation assists in the decision about risk treatment.
2.69 risk identification
process of finding, recognizing and describing risks (2.62)


NOTE 1 Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders’ needs.

2.70 risk management
coordinated activities to direct and control an organization with regard to risk (2.62)


2.71 risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing risk (2.62)


NOTE ISO/IEC 27005 uses the term ‘process’ to describe risk management overall. The elements within the risk management process are termed ‘activities’

2.72 risk treatment
process (2.55) to modify risk (2.62)


NOTE 1 Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
— taking or increasing risk in order to pursue an opportunity;
— removing the risk source;
— changing the likelihood;
— changing the consequences;
— sharing the risk with another party or parties (including contracts and risk financing); and
— retaining the risk by informed choice.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks.
2.73 scale
ordered set of values, continuous or discrete, or a set of categories to which the attribute (2.6) is mapped

[ISO/IEC 15939:2007]

NOTE The type of scale depends on the nature of the relationship between values on the scale. Four types of scale are commonly defined:

— nominal: the measurement values are categorical;
— ordinal: the measurement values are rankings;
— interval: the measurement values have equal distances corresponding to equal quantities of the attribute;
— ratio: the measurement values have equal distances corresponding to equal quantities of the attribute, where the value of zero corresponds to none of the attribute.

These are just examples of the types of scale.

2.74 security implementation standard
document specifying authorized ways for realizing security

2.75 stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity


2.76 statement of applicability
documented statement describing the control objectives (2.17) and controls (2.16) that are relevant and applicable to the organization’s ISMS (2.35)

2.77 third party
person or body that is recognized as being independent of the parties involved, as concerns the issue in question


2.78 threat
potential cause of an unwanted incident, which may result in harm to a system or organization

2.79 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

[ISO/IEC 15939:2007]
2.80 validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

2.81 verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2005]

NOTE This could also be called compliance testing.

2.82 vulnerability
weakness of an asset (2.4) or control (2.16) that can be exploited by one or more threats (2.78)

3 Information security management systems

3.1 Introduction

Organizations of all types and sizes:

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

b) recognise 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 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; and

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.

An organization's information is dependent upon information and communications
technology. This technology is an essential element in any organization and assists in
facilitating the creation, processing, storing, transmitting, protection and destruction of
information. Where the extent of the interconnected global business environment expands
so does the requirement to protect information as this information is now exposed to a
wider variety of threats and vulnerabilities.

3.2.3 Information security

Information security includes three main dimensions: confidentiality, availability and
integrity. Information security involves the application and management of appropriate
security measures that involves consideration of a wide range of threats, with the aim of
ensuring sustained business success and continuity, and minimising impacts of information
security breaches.

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

NOTE The term "management" may sometimes refer to people (i.e. a person or group of people with authority and
responsibility for the conduct and control of an organization). The term "management" addressed in this clause is not in
this sense.

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 and to the environment.

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”.

The process approach for the ISMS presented in the ISMS family of standards is based on the operating principle adopted in ISO’s management system standards commonly known as the Plan – Do – Check – Act (PDCA) process.

a) Plan – establish objectives and make plans (analyze the organization's situation, establish the overall objectives and set targets, and develop plans to achieve them);
b) Do – implement plans (do what was planned to do);
c) Check – measure results (measure/monitor the extent to which achievements meet planned objectives); and

d) Act – correct and improve activities (learn from mistakes to improve activities to achieve better results).

3.4 Why an ISMS is important

As part of an organization's ISMS, 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, 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 increases 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-recognisable 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 an information system after the fact could be cumbersome 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 information security risks 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 3.6.2);

b) assess information security risks (see 3.6.3);

c) select and implement relevant controls to manage unacceptable risks (see 3.6.4); and

d) monitor, maintain and improve the effectiveness of controls associated with the organization's information assets (see 3.6.5).

To ensure the ISMS is effectively protecting the organization's information assets on an ongoing basis, it is necessary for steps (a) – (d) to be continuously 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:

a) identified information assets and their value;

b) business needs for information processing and storage; and

c) legal, regulatory, and contractual requirements.

Conducting a methodical assessment of the risks associated with the organization's information assets will involve analyzing: 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 materialising.

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, e.g. 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. Furthermore, 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:

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) transferring the associated risks to other parties, e.g. 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 (see 3.6.2) have been identified and information security risks to the identified information assets have been determined and assessed (see 3.6.3), and decisions for the treatment of information security risks having been made (see 3.6.4), selection and implementation of controls apply for risk reduction.

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

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

b) organizational objectives;

c) operational requirements and constraints;

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

e) the need to balance the investment in implementation and operation of controls against the threat likely to result from information security events.
The controls specified in ISO/IEC 27002:2005 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.

Controls can be selected from this standard 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. 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.

It should be kept in mind that no set of controls can achieve complete information security, and that additional management action 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 organization policy 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.

3.6 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:

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; and

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 realised for an organization to achieve sustainable success from the adoption of the ISMS family of standards include:

a) a structured manner supporting the process of specifying, implementing, operating and maintaining a comprehensive, cost-effective and 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; and

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, either 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) and certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001. Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process, control-related guidelines as well as
sector-specific guidance. Relationships between the ISMS family of standards 2) are illustrated in Figure 1.

![Figure 1 — ISMS Family of Standards Relationships](image)

2 Standards that provide direct support, detailed guidance and/or interpretation for the overall PDCA processes and requirements specified in ISO/IEC 27001 (see 4.3.1) are: ISO/IEC 27000 (see 4.2.1), ISO/IEC 27002 (see 4.4.1), ISO/IEC 27003 (see 4.4.2), ISO/IEC 27004 (see 4.4.3), ISO/IEC 27005 (see 4.4.4), ISO/IEC 27007 (see 4.4.5), ISO/IEC 27013 (see 4.4.7), ISO/IEC 27014 (see 4.4.8) and ISO/IEC 27016 (see 4.4.9).

3 Standards that provide direct support, detailed guidance and/or interpretation for the controls specified in ISO/IEC 27002 (see 4.4.1) are: ISO/IEC 27008 (see 4.4.6).

4 ISO/IEC 27006 (see 4.3.2) addresses requirements of bodies providing ISMS certifications.

5 ISO/IEC 27010 (see 4.5.1), ISO/IEC 27011 (see 4.5.2), ISO/IEC 27015 (see 4.5.3) and ISO 27799 (4.5.4) addresses sector-specific guidelines for ISMS. 3)

2) ISO/IEC 27007 and 27008 are currently under development.

3) ISO/IEC 27009 is reserved for future standards associated with the ISMS family of standards that have not yet been defined when this International Standard was published.
The ISMS family of standards maintains relationships with many other ISO and ISO/IEC standards and are classified and further described as being either:

a) 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 document)

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

Purpose: ISO/IEC 27000 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 Annex A (ISO/IEC 27001) shall be selected as part of this ISMS process as appropriate to cover the identified requirements. The control objectives and controls listed in Table A.1 (ISO/IEC 27001) are directly derived from and aligned with those listed in ISO/IEC 27002 Clauses 5 to 15.
ISO/IEC 3rd WD 27000

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 management

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 15 provides specific implementation advice and guidance on best practice in support of the controls specified in Clauses A.5 to A.15 of ISO/IEC 27001.

4.4.2 ISO/IEC 27003

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

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

Purpose: ISO/IEC 27003 will provide 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 will provide 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.
1 **Purpose:** ISO/IEC 27004 will provide 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*

5 **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.

6 **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*

9 **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.

10 **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 27008**

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

13 **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.

14 **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, 27005 or 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 provides 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 adopted, or vice versa;
b) implement both ISO/IEC 27001 and ISO/IEC 20000-1 together;
c) align existing ISO/IEC 27001 and ISO/IEC 20000-1 management system (MS) implementations.

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 MS that conforms to both International Standards.

4.4.8 ISO/IEC 27014

Information technology — Security techniques — Governance of information security

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

Purpose: Information security has become a key issue for organisations. Not only are there increasing regulatory requirements but also the failure of an organisation's information security measures can have a direct impact on an organisation’s reputation. Therefore, governing body, 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 provides 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 determining the optimum level of resources to be applied in securing these information assets.

Purpose: This Technical Report supplements 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 provides 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 guidelines 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-organisational 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 organisation’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 Management (ISM) in telecommunications organizations.

Purpose: ISO/IEC 27011 provides telecommunications organisations 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.

4.5.3 ISO/IEC 27015

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

Scope: This International Standard provide guidelines in addition to the guidance
given in the ISO/IEC 27000 family of standards, for initiating, implementing, maintaining,
and improving information security within organisations providing financial services.

Purpose: This International Standard is a specialist supplement to ISO/IEC 27001 and
ISO/IEC 27002 International Standards for use by organisations providing financial services
to support them in:

a) Initiating, implementing, maintaining, and improving of an information security

b) Designing and implementing controls defined in the ISO/IEC 27002:2005
International Standard or within this International Standard.

4.5.4 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 (ISM) in health organizations.
Purpose: ISO/IEC 27799 provides health organisations 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 required 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.

<table>
<thead>
<tr>
<th>INDICATION</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement</td>
<td>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</td>
</tr>
<tr>
<td>Recommendation</td>
<td>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</td>
</tr>
<tr>
<td>Permission</td>
<td>the term “may” and “need not” indicates a course of action permissible within the limits of the document</td>
</tr>
<tr>
<td>Possibility</td>
<td>the term “can” and “cannot” indicates a possibility of something occurring</td>
</tr>
</tbody>
</table>
Bibliography


4) To be published.
5) To be published.
6) To be published.
ISO/IEC 27013\textsuperscript{7)}, \textit{Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1}

ISO/IEC 27014\textsuperscript{8)}, \textit{Information technology -- Security techniques – Governance of information security}

ISO/IEC 27015\textsuperscript{9)}, \textit{Information security management guidelines for financial services}

ISO/IEC 27016\textsuperscript{10)}, \textit{Information security management – Organizational economics}


---

\textsuperscript{7)} To be published.
\textsuperscript{8)} To be published.
\textsuperscript{9)} To be published.
\textsuperscript{10)} To be published.