INTERNATIONAL STANDARD

**ISO/IEC 27000**

Third edition
2014-01-15

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

*Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

Reference number
ISO/IEC 27000:2014(E)

# 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.

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 third edition cancels and replaces the second edition (ISO/IEC 27000:2012), which has been technically revised.

# 0 Introduction

## 0.1 Overview

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

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

## 0.2 ISMS family of standards

The ISMS family of standards (see Clause 4) is intended to assist organizations of all types and sizes to implement and operate an ISMS and consists of the following International Standards, under the general title *Information technology — Security techniques* (given below in numerical order):

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

— ISO/IEC 27001, *Information security management systems — Requirements*

— ISO/IEC 27002, *Code of practice for information security controls*

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

— ISO/IEC 27004, *Information security management — Measurement*

— ISO/IEC 27005, *Information security risk management*

— ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems*

— ISO/IEC 27007, *Guidelines for information security management systems auditing*

— ISO/IEC TR 27008, *Guidelines for auditors on information security controls*

— ISO/IEC 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*

NOTE The general title "*Information technology — Security techniques*" indicates that these standards were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:

— ISO 27799:2008, *Health informatics — Information security management in health using* ISO/IEC 27002

## 0.3 Purpose of this International Standard

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

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

The ISMS family of standards includes standards that:

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

b) provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain and improve an ISMS;

c) address sector-specific guidelines for ISMS; and

d) address conformity assessment for ISMS.

The terms and definitions provided in this International Standard:

— cover commonly used terms and definitions in the ISMS family of standards;

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

— do not limit the ISMS family of standards in defining new terms for use.

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

## 1 Scope

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

## 2 Terms and definitions

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

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

**2.2**
**analytical model**
algorithm or calculation combining one or more *base measures* (2.10) and/or *derived measures* (2.22) with associated decision criteria

**2.3**
**attack**
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

**2.4**
**attribute**
property or characteristic of an *object* (2.55) that can be distinguished quantitatively or qualitatively by human or automated means

[SOURCE: ISO/IEC 15939:2007, modified – "entity" has been replaced by "object" in the definition.]

**2.5**
**audit**
systematic, independent and documented *process* (2.61) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

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

[SOURCE: ISO 19011:2011]

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

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

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

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

[SOURCE: ISO/IEC 15939:2007]

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

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

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

**2.13**
**conformity**
fulfilment of a *requirement* (2.63)

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

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

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: An event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and in the context of information security is usually negative.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through knock-on effects.

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

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

[SOURCE: ISO Guide 73:2009]

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

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

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

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

**2.19**
**corrective action**
action to eliminate the cause of a *nonconformity* (2.53) and to prevent recurrence

**2.20**
**data**
collection of values assigned to *base measures* (2.10), *derived measures* (2.22) and/or *indicators* (2.30)

[SOURCE: ISO/IEC 15939:2007]

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

**2.21**
**decision criteria**
thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result

[SOURCE: ISO/IEC 15939:2007]

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

[SOURCE: ISO/IEC 15939:2007]

**2.23**
**documented information**
information required to be controlled and maintained by an *organization* (2.57) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to

— the *management system* (2.46), including related *processes* (2.61);

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

— evidence of results achieved (records).

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

**2.25**
**event**
occurrence or change of a particular set of circumstances

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: An event can be one or more occurrences, and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”.

**2.26**
**executive management**
person or group of people who have delegated responsibility from the *governing body* (2.29) for implementation of strategies and policies to accomplish the purpose of the *organization* (2.57)

Note 1 to entry: Executive management is sometimes called top management and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles

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

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: External context can include:

— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having impact on the *objectives* (2.56) of the *organization* (2.57); and

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

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

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

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

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

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

[SOURCE: ISO/IEC 15939:2007]

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

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

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

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

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

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

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

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

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

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

**2.40**
**integrity**
property of accuracy and completeness

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

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

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: Internal context can include:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

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

— relationships with, and perceptions and values of, internal stakeholders;

— the organization's culture;

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

— form and extent of contractual relationships.

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

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

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

**2.45**
**likelihood**
chance of something happening

[SOURCE: ISO Guide 73:2009]

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

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

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

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

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

[SOURCE: ISO/IEC 15939:2007]

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

**2.48**
**measurement**
*process* (2.61) to determine a value

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

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

[SOURCE: ISO/IEC 15939:2007]

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

[SOURCE: ISO/IEC 15939:2007]

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

— subjective: quantification involving human judgment;

— objective: quantification based on numerical rules.

**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 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 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 management systems, information security objectives are set by the organization, consistent with the information security policy, 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 o*bjectives* (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 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 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 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.

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

Note 1 to entry: Residual risk can contain unidentified risk.

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

[SOURCE: ISO Guide 73:2009]

**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

**2.68**
**risk**
effect of uncertainty on objectives

[SOURCE: ISO Guide 73:2009]

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 (including changes in circumstances) and the associated likelihood (2.45) of occurrence.

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

Note 6 to entry: Information security 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.

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

[SOURCE: ISO Guide 73:2009]

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

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

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

[SOURCE: ISO Guide 73:2009]

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]

**2.72**
**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* (2.82) regarding the management of *risk* (2.68)

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

Note 2 to entry: 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.

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

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: Risk criteria are based on organizational objectives, and external and internal context.

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.

**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]

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

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

[SOURCE: ISO Guide 73:2009]

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

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' 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]

**2.77**
**risk management process**
systematic application of management policies, 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]

Note 1 to entry: ISO/IEC 27005 uses the term 'process' to describe risk management overall. The elements within the risk management process 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]

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

[SOURCE: ISO Guide 73:2009]

Note 1 to entry: 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 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

Note 3 to entry: Risk treatment can create new risks or modify existing risks.

**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]

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:

— 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.

**2.81**
**security implementation standard**
document specifying authorized ways for realizing security

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

[SOURCE: ISO Guide 73:2009]

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

**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.

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 supporting information exchange within an information sharing community

**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]

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

[SOURCE: ISO 9000:2005]

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

[SOURCE: ISO 9000:2005]

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 Introduction

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; 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.

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 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 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, 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-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); and

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) – (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:

a) identified information assets and their value;

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

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 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. 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) sharing 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 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 having 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 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) they 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.

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:

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

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; 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, 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[1)] are illustrated in Figure 1.

1) The development or revision status of any standard can be established by reference to http://www.iso.org/iso/home.html and searching for the standard of interest.

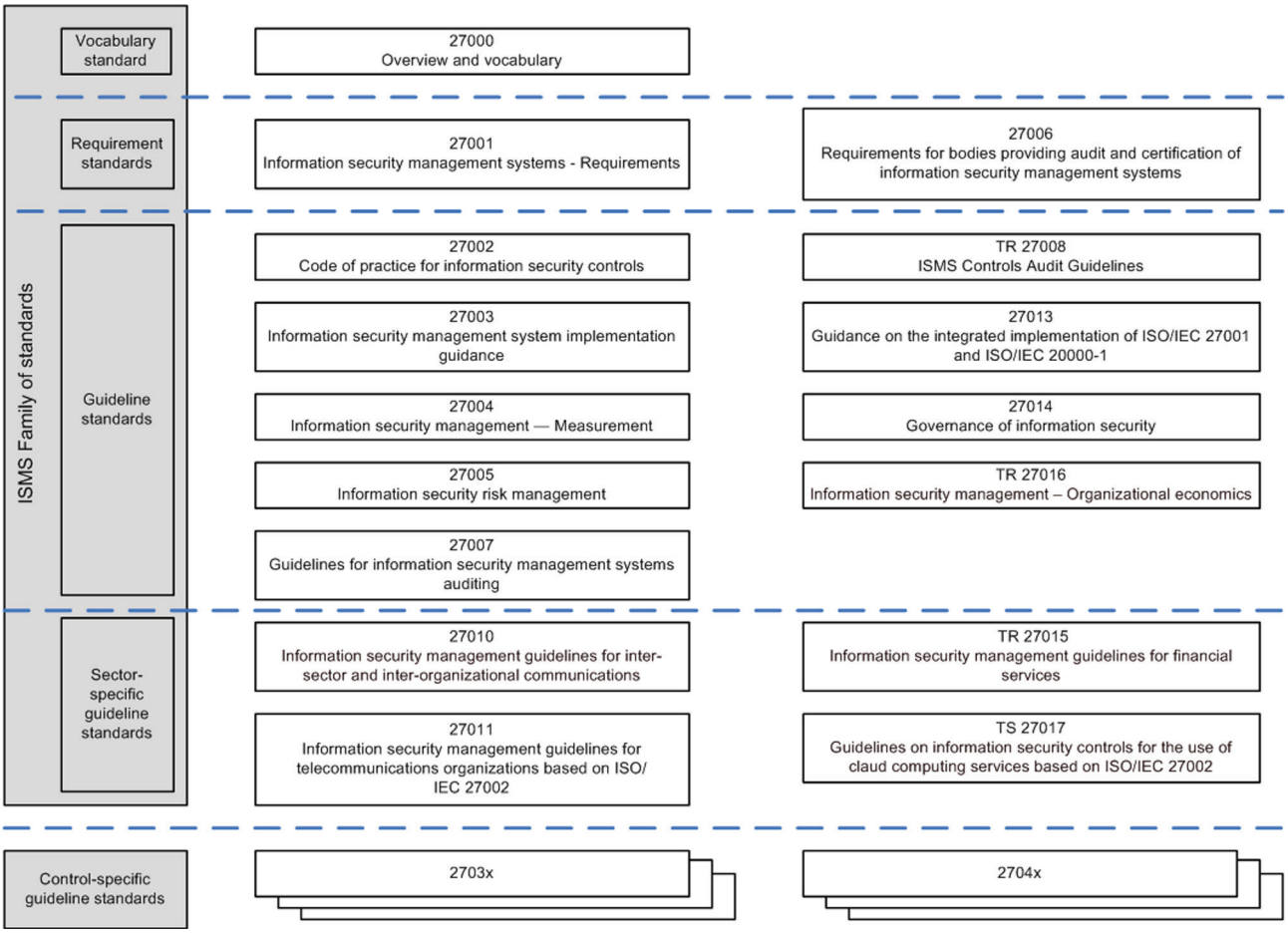


**Figure 1 — ISMS Family of Standards Relationships**

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 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 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 Clauses A.5 to A.18 of ISO/IEC 27001.

### 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:

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 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 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 Management in telecommunications organizations.

**Purpose:** ISO/IEC 27011 provides telecommunications 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.

### 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 International Standards 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 the ISO/IEC 27001:2005 International Standard.

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 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, *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 ordered by Standards

### B.2.1 ISO/IEC 27001

| | | | |
|---|---|---|---|
| audit | 2.5 | measurement | 2.48 |
| availability | 2.9 | monitoring | 2.52 |
| competence | 2.11 | non-conformity | 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

| | |
|---|---|
| certificate | mark |
| certification body | organization |
| certification document | |

### B.2.7 ISO/IEC 27007

| | |
|---|---|
| audit scope | 2.6 |

### B.2.8 ISO/IEC TR 27008

| | | | |
|---|---|---|---|
| review object | 2.66 | security implementation standard | 2.81 |
| review objective | 2.67 | | |

### 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 | governing body | 2.29 |
| governance of information security | 2.28 | stakeholder | 2.82 |

### B.2.12 ISO/IEC TR 27015

financial services

### B.2.13 ISO/IEC TR 27016

annualized loss expectancy ALE

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

loss

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

# Bibliography


[1] ISO/IEC 17021:2011, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[2] ISO 9000:2005, *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 27003:2010, *Information technology — Security techniques — Information security management system implementation guidance*

[7] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*

[8] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

[9] ISO/IEC 27006:2011, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[10] ISO/IEC 27007:2011, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[11] ISO/IEC TR 27008:2011, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[12] ISO/IEC 27010:2012, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[13] ISO/IEC 27011:2008, *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[14] ISO/IEC 27013:2012, *Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

[15] ISO/IEC 27014:2013, *Information technology — Security techniques — Governance of information security*

[16] ISO/IEC TR 27015:2012, *Information technology — Security techniques — Information security management guidelines for financial services*

[17] ISO/IEC TR 27016:—[2)], *Information technology — Security techniques — Information security management — Organizational economics*

[18] ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

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

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


2) Awaiting publication.

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

**ICS 01.040.35;35.040**
Price based on 31 pages