INTERNATIONAL STANDARD

ISO/IEC 27000

Fifth edition
2018-02

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 27000:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This fifth edition cancels and replaces the fourth edition (ISO/IEC 27000:2016), which has been technically revised. The main changes compared to the previous edition are as follows:

— the Introduction has been reworded;

— some terms and definitions have been removed;

— Clause 3 has been aligned on the high-level structure for MSS;

— Clause 5 has been updated to reflect the changes in the standards concerned;

— Annexes A and B have been deleted.

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 Purpose of this document

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.

0.3 Content of this document

In this document, the following verbal forms are used:

— “shall” indicates a requirement;

— “should” indicates a recommendation;

— “may” indicates a permission;

— “can” indicates a possibility or a capability.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirement. “Notes to entry” used in Clause 3 provide additional information that supplements the terminological data and can contain provisions relating to the use of a term.

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

1 Scope

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

The terms and definitions provided in this document

— 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.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
access control
means to ensure that access to assets is authorized and restricted based on business and security *requirements* (3.56)

3.2
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

3.3
audit
systematic, independent and documented *process* (3.54) 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: An internal audit is conducted by the organization itself, or by an external party on its behalf.

Note 3 to entry: “Audit evidence” and “audit criteria” are defined in ISO 19011.

3.4
audit scope
extent and boundaries of an *audit* (3.3)

[SOURCE: ISO 19011:2011, 3.14, modified — Note 1 to entry has been deleted.]

3.5
authentication
provision of assurance that a claimed characteristic of an entity is correct

3.6
authenticity
property that an entity is what it claims to be

3.7
availability
property of being accessible and usable on demand by an authorized entity

3.8
base measure
measure (3.42) defined in terms of an attribute and the method for quantifying it

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

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.3, modified — Note 2 to entry has been deleted.]

3.9
competence
ability to apply knowledge and skills to achieve intended results

3.10
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or *processes* (3.54)

3.11
conformity
fulfilment of a *requirement* (3.56)

3.12
consequence
outcome of an *event* (3.21) affecting *objectives* (3.49)

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.

[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified — Note 2 to entry has been changed after “and”.]

3.13
continual improvement
recurring activity to enhance *performance* (3.52)

3.14
control
measure that is modifying *risk* (3.61)

Note 1 to entry: Controls include any *process* (3.54), *policy* (3.53), device, practice, or other actions which modify *risk* (3.61).

Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect.

[SOURCE: ISO Guide 73:2009, 3.8.1.1 — Note 2 to entry has been changed.]

3.15
control objective
statement describing what is to be achieved as a result of implementing *controls* (3.14)

3.16
correction
action to eliminate a detected *nonconformity* (3.47)

3.17
corrective action
action to eliminate the cause of a *nonconformity* (3.47) and to prevent recurrence

3.18
derived measure
measure (3.42) that is defined as a function of two or more values of *base measures* (3.8)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.8, modified — Note 1 to entry has been deleted.]

3.19
documented information
information required to be controlled and maintained by an *organization* (3.50) 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* (3.41), including related *processes* (3.54);

— information created in order for the *organization* (3.50) to operate (documentation);

— evidence of results achieved (records).

3.20
effectiveness
extent to which planned activities are realized and planned results achieved

3.21
event
occurrence or change of a particular set of circumstances

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".

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — Note 4 to entry has been deleted.]

3.22
external context
external environment in which the organization seeks to achieve its *objectives* (3.49)

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

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

— key drivers and trends having impact on the *objectives* of the *organization* (3.50);

— relationships with, and perceptions and values of, external *stakeholders* (3.37).

[SOURCE: ISO Guide 73:2009, 3.3.1.1]

3.23
governance of information security
system by which an *organization's* (3.50) *information security* (3.28) activities are directed and controlled

3.24
governing body
person or group of people who are accountable for the *performance* (3.52) and conformity of the *organization* (3.50)

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

3.25
indicator
measure (3.42) that provides an estimate or evaluation

3.26
information need
insight necessary to manage *objectives* (3.49), goals, risks and problems

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.12]

3.27
information processing facilities
any information processing system, service or infrastructure, or the physical location housing it

3.28
information security
preservation of *confidentiality* (3.10), *integrity* (3.36) and *availability* (3.7) of information

Note 1 to entry: In addition, other properties, such as *authenticity* (3.6), accountability, *non-repudiation* (3.48), and *reliability* (3.55) can also be involved.

3.29
information security continuity
processes (3.54) and procedures for ensuring continued *information security* (3.28) operations

3.30
information security event
identified occurrence of a system, service or network state indicating a possible breach of *information security* (3.28) *policy* (3.53) or failure of *controls* (3.14), or a previously unknown situation that can be security relevant

3.31
information security incident
single or a series of unwanted or unexpected *information security events* (3.30) that have a significant probability of compromising business operations and threatening *information security* (3.28)

3.32
information security incident management
set of *processes* (3.54) for detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.31)

3.33
information security management system (ISMS) professional
person who establishes, implements, maintains and continuously improves one or more information security management system *processes* (3.54)

3.34
information sharing community
group of *organizations* (3.50) that agree to share information

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

3.35
information system
set of applications, services, information technology assets, or other information-handling components

3.36
integrity
property of accuracy and completeness

3.37
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.50) that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.38
internal context
internal environment in which the *organization* (3.50) seeks to achieve its objectives

Note 1 to entry: Internal context can include:

— governance, organizational structure, roles and accountabilities;

— *policies* (3.53), *objectives* (3.49), 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* (3.54), systems and technologies);

— *information systems* (3.35), information flows and decision-making *processes* (both formal and informal);

— relationships with, and perceptions and values of, internal *stakeholders* (3.37);

— the organization's culture;

— standards, guidelines and models adopted by the organization;

— form and extent of contractual relationships.

[SOURCE: ISO Guide 73:2009, 3.3.1.2]

3.39
level of risk
magnitude of a *risk* (3.61) expressed in terms of the combination of *consequences* (3.12) and their *likelihood* (3.40)

[SOURCE: ISO Guide 73:2009, 3.6.1.8, modified — "or combination of risks" has been deleted in the definition.]

3.40
likelihood
chance of something happening

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

3.41
management system
set of interrelated or interacting elements of an *organization* (3.50) to establish *policies* (3.53) and *objectives* (3.49) and *processes* (3.54) 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 and operation.

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.

3.42
measure
variable to which a value is assigned as the result of *measurement* (3.43)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.15, modified — Note 2 to entry has been deleted.]

3.43
measurement
process (3.54) to determine a value

3.44
measurement function
algorithm or calculation performed to combine two or more *base measures* (3.8)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.20]

3.45
measurement method
logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale

Note 1 to entry: The type of measurement method depends on the nature of the operations used to quantify an *attribute* (3.4). Two types can be distinguished:

— subjective: quantification involving human judgment; and

— objective: quantification based on numerical rules.

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.21, modified — Note 2 to entry has been deleted.]

3.46
monitoring
determining the status of a system, a *process* (3.54) or an activity

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

3.47
nonconformity
non-fulfilment of a *requirement* (3.56)

3.48
non-repudiation
ability to prove the occurrence of a claimed *event* (3.21) or action and its originating entities

3.49
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* (3.54)].

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.

3.50
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.49)

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.

3.51
outsource
make an arrangement where an external *organization* (3.50) performs part of an organization's function or *process* (3.54)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.41), although the outsourced function or process is within the scope.

3.52
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* (3.54), products (including services), systems or *organizations* (3.50).

3.53
policy
intentions and direction of an *organization* (3.50), as formally expressed by its *top management* (3.75)

3.54
process
set of interrelated or interacting activities which transforms inputs into outputs

3.55
reliability
property of consistent intended behaviour and results

3.56
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.

3.57
residual risk
risk (3.61) remaining after *risk treatment* (3.72)

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

Note 2 to entry: Residual risk can also be referred to as “retained risk”.

3.58
review
activity undertaken to determine the suitability, adequacy and *effectiveness* (3.20) of the subject matter to achieve established *objectives* (3.49)

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

3.59
review object
specific item being reviewed

3.60
review objective
statement describing what is to be achieved as a result of a *review* (3.59)

3.61
risk
effect of uncertainty on *objectives* (3.49)

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, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73:2009, 3.5.1.3) and “consequences” (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” (as defined in ISO Guide 73:2009, 3.6.1.1) 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 will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

3.62
risk acceptance
informed decision to take a particular *risk* (3.61)

Note 1 to entry: Risk acceptance can occur without *risk treatment* (3.72) or during the *process* (3.54) of risk treatment.

Note 2 to entry: Accepted risks are subject to *monitoring* (3.46) and *review* (3.58).

[SOURCE: ISO Guide 73:2009, 3.7.1.6]

3.63
risk analysis
process (3.54) to comprehend the nature of *risk* (3.61) and to determine the *level of risk* (3.39)

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (3.67) and decisions about *risk treatment* (3.72).

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO Guide 73:2009, 3.6.1]

3.64
risk assessment
overall *process* (3.54) of *risk identification* (3.68), *risk analysis* (3.63) and *risk evaluation* (3.67)

[SOURCE: ISO Guide 73:2009, 3.4.1]

3.65
risk communication and consultation
set of continual and iterative *processes* (3.54) that an organization conducts to provide, share or obtain information, and to engage in dialogue with *stakeholders* (3.37) regarding the management of *risk* (3.61)

Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (3.41), significance, evaluation, acceptability and treatment of risk.

Note 2 to entry: Consultation is a two-way process of informed communication between an *organization* (3.50) 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.

3.66
risk criteria
terms of reference against which the significance of *risk* (3.61) is evaluated

Note 1 to entry: Risk criteria are based on organizational objectives, and *external context* (3.22) and *internal context* (3.38).

Note 2 to entry: Risk criteria can be derived from standards, laws, *policies* (3.53) and other *requirements* (3.56).

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

3.67
risk evaluation
process (3.54) of comparing the results of *risk analysis* (3.63) with *risk criteria* (3.66) to determine whether the *risk* (3.61) and/or its magnitude is acceptable or tolerable

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (3.72).

[SOURCE: ISO Guide 73:2009, 3.7.1]

3.68
risk identification
process (3.54) of finding, recognizing and describing *risks* (3.61)

Note 1 to entry: Risk identification involves the identification of risk sources, *events* (3.21), their causes and their potential *consequences* (3.12).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and *stakeholders'* (3.37) needs.

[SOURCE: ISO Guide 73:2009, 3.5.1]

3.69
risk management
coordinated activities to direct and control an *organization* (3.50) with regard to *risk* (3.61)

[SOURCE: ISO Guide 73:2009, 2.1]

3.70
risk management process
systematic application of management *policies* (3.53), procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing *risk* (3.61)

Note 1 to entry: ISO/IEC 27005 uses the term "*process*" (3.54) to describe risk management overall. The elements within the *risk management* (3.69) process are referred to as "activities".

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

3.71
risk owner
person or entity with the accountability and authority to manage a *risk* (3.61)

[SOURCE: ISO Guide 73:2009, 3.5.1.5]

3.72
risk treatment
process (3.54) to modify *risk* (3.61)

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* (3.40);

— changing the *consequences* (3.12);

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

— 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.

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

3.73
security implementation standard
document specifying authorized ways for realizing security

3.74
threat
potential cause of an unwanted incident, which can result in harm to a system or *organization* (3.50)

3.75
top management
person or group of people who directs and controls an *organization* (3.50) 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* (3.41) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

Note 3 to entry: Top management is sometimes called executive management and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles.

3.76
trusted information communication entity
autonomous *organization* (3.50) supporting information exchange within an *information sharing community* (3.34)

3.77
vulnerability
weakness of an asset or *control* (3.14) that can be exploited by one or more *threats* (3.74)

4 Information security management systems

4.1 General

Organizations of all types and sizes:

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

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

c) face a range of risks that can 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.

4.2 What is an ISMS?

4.2.1 Overview and principles

An 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 on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:

a) awareness of the need for information security;

b) assignment of responsibility for information security;

c) incorporating management commitment and the interests of stakeholders;

d) enhancing societal values;

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

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

g) active prevention and detection of information security incidents;

h) ensuring a comprehensive approach to information security management;

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

4.2.2 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 can be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which it is transmitted, it always needs appropriate protection.

In many organizations, information is dependent on 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.

4.2.3 Information security

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

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

4.2.4 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.

4.2.5 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.

4.3 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".

4.4 Why an ISMS is important

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

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

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

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

An ISMS is important to both public and private sector businesses. In any industry, an ISMS is an enabler that supports e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increase the difficulty of controlling

access to and handling of information. In addition, the distribution of mobile storage devices containing information assets can weaken the effectiveness of traditional controls. When organizations adopt the ISMS family of standards, the ability to apply consistent and mutually-recognizable information security principles can be demonstrated to business partners and other interested parties.

Information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the information security that can be achieved through technical means is limited, and can be ineffective without being supported by appropriate management and procedures within the context of an ISMS. Integrating security into a functionally complete information system can 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 can 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.

4.5 Establishing, monitoring, maintaining and improving an ISMS

4.5.1 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 4.5.2);

b) assess information security risks (see 4.5.3) and treat information security risks (see 4.5.4);

c) select and implement relevant controls to manage unacceptable risks (see 4.5.5);

d) monitor, maintain and improve the effectiveness of controls associated with the organization's information assets (see 4.5.6).

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

4.5.2 Identifying information security requirements

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

a) identified information assets and their value;

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

c) legal, regulatory, and contractual requirements.

Conducting a methodical assessment of the risks associated with the organization's information assets involves analysing threats to information assets, vulnerabilities to and the likelihood of a threat

materializing to information assets, and the potential impact of any information security incident on information assets. The expenditure on relevant controls is expected to be proportionate to the perceived business impact of the risk materializing.

4.5.3 Assessing information security risks

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

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

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

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

4.5.4 Treating information security risks

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

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

a) applying appropriate controls to reduce the risks;

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

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

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

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

4.5.5 Selecting and implementing controls

Once information security requirements have been identified (see 4.5.2), information security risks to the identified information assets have been determined and assessed (see 4.5.3) and decisions for the

treatment of information security risks have been made (see 4.5.4), then selection and implementation of controls for risk reduction apply.

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

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

b) organizational objectives;

c) operational requirements and constraints;

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

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

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

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

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, in the worst case, inability to achieve adequate security. Controls can be selected from ISO/IEC 27002 or from other control sets. Alternatively, new controls can be designed to meet the specific needs of the organization. It is necessary to recognize the possibility that some controls not be applicable to every information system or environment, and not be practicable for all organizations.

Sometimes, implementing a chosen set of controls takes time and, during that time, the level of risk can 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.

4.5.6 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 checks 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 provides evidence of verification and traceability of corrective, preventive and improvement actions.

4.5.7 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.

4.6 ISMS critical success factors

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

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

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

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

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

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

f) an effective information security incident management process;

g) an effective business continuity management approach;

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

An ISMS increases the likelihood of an organization consistently achieving the critical success factors required to protect its information assets.

4.7 Benefits of the ISMS family of standards

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

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

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

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

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

e) increase in stakeholder trust in the organization;

f) satisfying societal needs and expectations;

g) more effective economic management of information security investments.

5 ISMS family of standards

5.1 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 on:

— standards describing ISMS requirements (ISO/IEC 27001);

— certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001; and

— additional requirement framework for sector-specific implementations of the ISMS (ISO/IEC 27009).

Other documents provide guidance for various aspects of an ISMS implementation, addressing a generic process as well as sector-specific guidance.

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

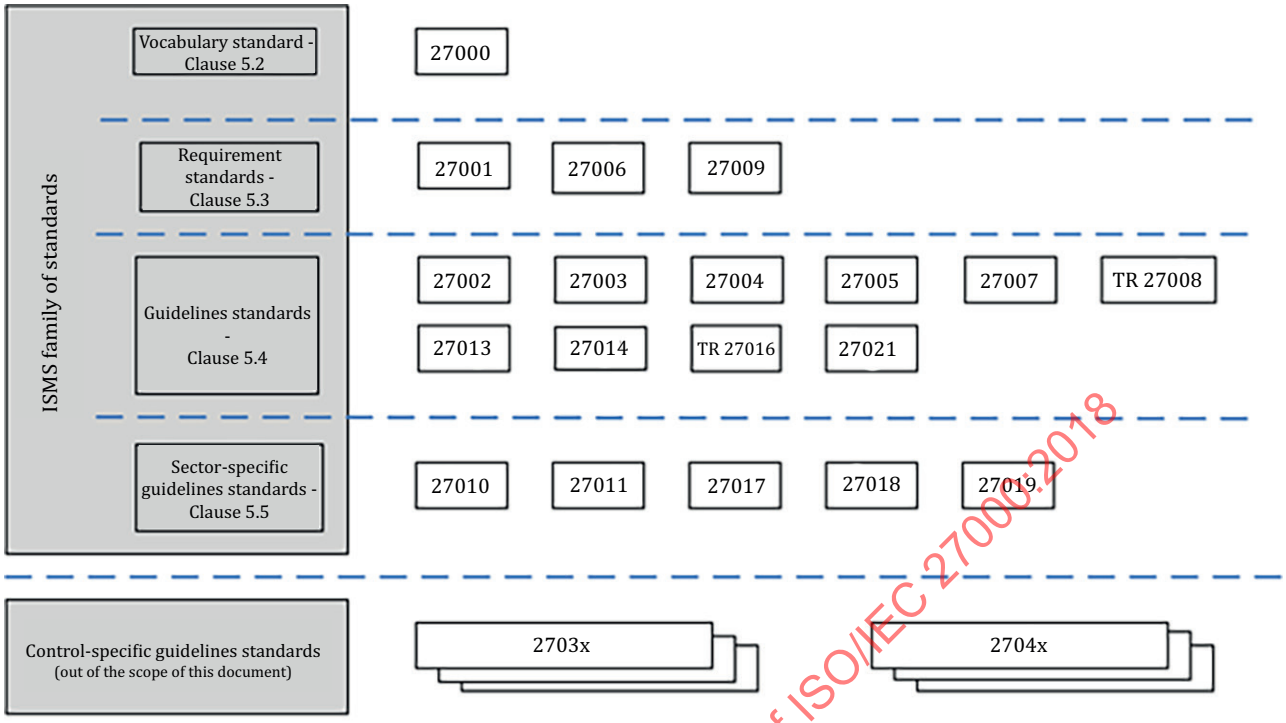

Figure 1 — ISMS family of standards relationships

Each of the ISMS family standards is described below by its type (or role) within the ISMS family of standards and its reference number.

5.2 Standard describing an overview and terminology: ISO/IEC 27000 (this document)

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

Scope: This document provides to organizations and individuals:

a) an overview of the ISMS family of standards;

b) an introduction to information security management systems; and

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

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

5.3 Standards specifying requirements

5.3.1 ISO/IEC 27001

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

Scope: This document 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 document can be used by all organizations, regardless of type, size and nature.

Purpose: ISO/IEC 27001 provides normative requirements for the development and operation of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. Organizations operating an ISMS may have its conformity audited and certified. The control objectives and controls from ISO/IEC 27001:2013, Annex A shall be selected as part of this ISMS process as appropriate to cover the identified requirements. The control objectives and controls listed in ISO/IEC 27001:2013, Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013, Clauses 5 to 18.

5.3.2 ISO/IEC 27006

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

Scope: This document 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.

The requirements contained in this document need to be demonstrated in terms of competence and reliability by anybody providing ISMS certification, and the guidance contained in this document provides additional interpretation of these requirements for anybody providing ISMS certification.

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.

5.3.3 ISO/IEC 27009

Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

Scope: This document defines the requirements for the use of ISO/IEC 27001 in any specific sector (field, application area or market sector). It explains how to include requirements additional to those in ISO/IEC 27001, how to refine any of the ISO/IEC 27001 requirements, and how to include controls or control sets in addition to ISO/IEC 27001:2013, Annex A.

Purpose: ISO/IEC 27009 ensures that additional or refined requirements are not in conflict with the requirements in ISO/IEC 27001.

5.4 Standards describing general guidelines

5.4.1 ISO/IEC 27002

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

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

Purpose: ISO/IEC 27002 provides guidance on the implementation of information security controls. Specifically, Clauses 5 to 18 provide specific implementation advice and guidance on best practice in support of the controls specified in ISO/IEC 27001:2013, A.5 to A.18.

5.4.2 ISO/IEC 27003

Information technology — Security techniques — Information security management —Guidance

Scope: This document provides explanation and guidance on ISO/IEC 27001:2013.

Purpose: ISO/IEC 27003 provides a background to the successful implementation of the ISMS in accordance with ISO/IEC 27001.

5.4.3 ISO/IEC 27004

Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

Scope: This document provides guidelines intended to assist organizations to evaluate the information security performance and the effectiveness of the ISMS in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It addresses:

a) the monitoring and measurement of information security performance;

b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls;

c) the analysing and the evaluating of the results of monitoring and measurement.

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

5.4.4 ISO/IEC 27005

Information technology — Security techniques — Information security risk management

Scope: This document provides guidelines for information security risk management. The approach described within this document 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.

5.4.5 ISO/IEC 27007

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

Scope: This document 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.

5.4.6 ISO/IEC TR 27008

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

Scope: This document 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 document 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 documentis not intended for management systems audits.