INTERNATIONAL STANDARD

ISO/IEC 27000

Second edition
2012-12-01

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 27000:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organisation 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 organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

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

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

0 Introduction

0.1 Overview

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

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

0.2 ISMS family of standards

The ISMS family of standards[1] (see Clause 4) is intended to assist organisations 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 27000:2009, *Information security management systems — Overview and vocabulary*

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

— ISO/IEC 27002:2005, *Code of practice for information security management*

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

— ISO/IEC 27004:2009, *Information security management — Measurement*

— ISO/IEC 27005:2011, *Information security risk management*

— ISO/IEC 27006:2011, *Requirements for bodies providing audit and certification of information security management systems*

— ISO/IEC 27007:2011, *Guidelines for information security management systems auditing*

— ISO/IEC TR 27008:2011, *Guidelines for auditors on information security management systems controls*

— ISO/IEC 27010:2012, *Information security management guidelines for inter-sector and inter-organisational communications*

— ITU-T X.1051 | ISO/IEC 27011:2008, *Information security management guidelines for telecommunications organisations based on ISO/IEC 27002*

— ISO/IEC FDIS 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

— ITU-T X.1054 | ISO/IEC FDIS 27014, Governance of information security

[1] Standards identified throughout this subclause with no release year indicated are still under development.

- ISO/IEC TR 27015, *Information security management guidelines for financial services*
- ISO/IEC WD 27016, *Information security management – Organisational 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 Plan-Do-Check-Act (PDCA) processes and requirements;

c) address sector-specific guidelines for ISMS; and

d) address conformity assessment for ISMS.

The terms and definitions provided in this International Standard:

- cover commonly used terms and definitions in the ISMS family of standards;
- will not cover all terms and definitions applied within the ISMS family of standards; and

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

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

1 Scope

This International Standard describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family of standards, and defines related terms and definitions.

This International Standard is applicable to all types and sizes of organisation (e.g. commercial enterprises, government agencies, not-for-profit organisations).

2 Terms and definitions

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

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

For example:

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

asset is defined as “any item that has value to the organisation”.

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

attack then becomes “attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of any item that has value to the organisation”.

2.1
access control
means to ensure that access to **assets** (2.4) is authorized and restricted based on business and security requirements

2.2
accountability
assignment of actions and decisions to an entity

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

[ISO/IEC 15939:2007]

2.4
asset
anything that has value to the organisation

NOTE There are many types of assets, including:

a) information;

b) software, such as a computer program;

c) physical, such as computer;

d) services;

e) people, and their qualifications, skills, and experience; and

f) intangibles, such as reputation and image.

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

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

[ISO/IEC 15939:2007]

2.7
audit scope
extent and boundaries of an audit

[ISO 9000:2005]

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

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

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

2.11
base measure
measure (2.43) defined in terms of an **attribute** (2.6) and the method for quantifying it

[ISO/IEC 15939:2007]

NOTE A base measure is functionally independent of other measures.

2.12
business continuity
procedures (2.53) and/or **processes** (2.54) for ensuring continued business operations

2.13
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or **processes** (2.54)

2.14
conformity
fulfillment of a requirement

[ISO 9000:2005].

NOTE The term “conformance” is synonymous but deprecated.

2.15
consequence
outcome of an **event** (2.24) affecting objectives

[ISO Guide 73:2009]

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

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

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

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

2.16
control
means of managing **risk** (2.61), including **policies** (2.51), **procedures** (2.53), **guidelines** (2.26), practices or organisational structures, which can be of administrative, technical, management, or legal nature

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

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

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

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

2.18
corrective action
action to eliminate the cause of a detected **non-conformity** (2.48) or other undesirable situation

[ISO 9000:2005]

2.19
data
collection of values assigned to **base measures** (2.11), **derived measures** (2.21) and/or **indicators** (2.27)

[ISO/IEC 15939:2007]

NOTE This definition applies only within the context of ISO/IEC 27004:2009.

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

[ISO/IEC 15939:2007]

2.21
derived measure
measure (2.43) that is defined as a function of two or more values of **base measures** (2.11)

[ISO/IEC 15939:2007]

2.22
effectiveness
extent to which planned activities are realized and planned results achieved

[ISO 9000:2005]

2.23
efficiency
relationship between the results achieved and the resources used

[ISO 9000:2005]

2.24
event
occurrence or change of a particular set of circumstances

[ISO Guide 73:2009]

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

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

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

[ISO Guide 73:2009]

NOTE External context can include:

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organisation; and
- relationships with, and perceptions and values of, external stakeholders.

2.26
guideline
description that clarifies what should be done and how, to achieve the objectives set out in **policies** (2.51)

2.27
indicator
measure (2.43) that provides an estimate or evaluation of specified **attributes** (2.6) derived from an **analytical model** (2.3) with respect to defined **information needs** (2.28)

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

[ISO/IEC 15939:2007]

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

2.30
information security
preservation of **confidentiality** (2.13), **integrity** (2.36) and **availability** (2.10) of information

NOTE In addition, other properties, such as **authenticity** (2.9), **accountability** (2.2), **non-repudiation** (2.49), and **reliability** (2.56) can also be involved.

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

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

2.33
information security incident management
processes (2.54) for detecting, reporting, assessing, responding to, dealing with, and learning from **information security incidents** (2.32)

2.34
information security management system
ISMS
part of the overall **management system** (2.42), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve **information security** (2.30)

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

2.35
information system
application, service, information technology asset, or any other information handling component

2.36
integrity
property of protecting the accuracy and completeness of **assets** (2.4)

2.37
internal context
internal environment in which the organisation seeks to achieve its objectives

[ISO Guide 73:2009]

NOTE Internal context can include:

- governance, organisational 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 organisation's culture;
- standards, guidelines and models adopted by the organisation; and
- form and extent of contractual relationships.

2.38
ISMS project
structured activities undertaken by an organisation to implement an **ISMS** (2.34)

2.39
level of risk
magnitude of a **risk** (2.61) expressed in terms of the combination of **consequences** (2.15) and their **likelihood** (2.40)

[ISO Guide 73:2009]

2.40
likelihood
chance of something happening

[ISO Guide 73:2009]

2.41
management
coordinated activities to direct and control an organisation

[ISO 9000:2005]

2.42
management system
framework of **guidelines** (2.26), **policies** (2.51), **procedures** (2.53), **processes** (2.54) and associated resources aimed at ensuring an organisation meets its objectives

2.43
measure
variable to which a value is assigned as the result of **measurement** (2.44)

[ISO/IEC 15939:2007]

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

2.44
measurement
process of obtaining information about the **effectiveness** (2.22) of **ISMS** (2.34) and **controls** (2.16) using a **measurement method** (2.46), a **measurement function** (2.45), an **analytical model** (2.3), and **decision criteria** (2.20)

2.45
measurement function
algorithm or calculation performed to combine two or more **base measures** (2.11)

[ISO/IEC 15939:2007]

2.46
measurement method
logical sequence of operations, described generically, used in quantifying an **attribute** (2.6) with respect to a specified **scale** (2.72)

[ISO/IEC 15939:2007]

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

- subjective: quantification involving human judgment;
- objective: quantification based on numerical rules.

2.47
measurement results
one or more **indicators** (2.27) and their associated interpretations that address an **information need** (2.28)

2.48
non-conformity
non-fulfillment of a requirement

[ISO 9000:2005]

2.49
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

2.50
object
item characterized through the **measurement** (2.44) of its **attributes** (2.6)

2.51
policy
overall intention and direction as formally expressed by **management** (2.41)

2.52
preventive action
action to eliminate the cause of a potential **non-conformity** (2.48) or other undesirable potential situation

[ISO 9000:2005]

2.53
procedure
specified way to carry out an activity or a **process** (2.54)

[ISO 9000:2005]

2.54
process
set of interrelated or interacting activities which transforms inputs into outputs

[ISO 9000:2005]

2.55
record
document stating results achieved or providing evidence of activities performed

[ISO 9000:2005]

2.56
reliability
property of consistent intended behaviour and results

2.57
residual risk
risk (2.61) remaining after **risk treatment** (2.71)

NOTE 1 Residual risk can contain unidentified risk.

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

2.58
review
activity undertaken to determine the suitability, adequacy and effectiveness (2.22) of the subject matter to achieve established objectives

[ISO 9000:2005]

2.59
review object
specific item being reviewed

2.60
review objective
statement describing what is to be achieved as a result of a review

2.61
risk
effect of uncertainty on objectives

[ISO Guide 73:2009]

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

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

NOTE 3 Risk is often characterized by reference to potential **events** (2.24) and **consequences** (2.15), or a combination of these.

NOTE 4 Information security risk is often expressed in terms of a combination of the consequences of an information security event and the associated **likelihood** (2.40) of occurrence.

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

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

2.62
risk acceptance
decision to accept a **risk** (2.61)

2.63
risk analysis
process to comprehend the nature of **risk** (2.61) and to determine the **level of risk** (2.39)

[ISO Guide 73:2009]

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

NOTE 2 Risk analysis includes risk estimation.

2.64
risk assessment
overall **process** (2.54) of **risk identification** (2.68), **risk analysis** (2.63) and **risk evaluation** (2.67)

[ISO Guide 73:2009]

2.65
risk communication and consultation
continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with **stakeholders** (2.74) regarding the management of **risk** (2.61)

[ISO Guide 73:2009]

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

NOTE 2 Consultation is a two-way process of informed communication between an organisation 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.

2.66
risk criteria
terms of reference against which the significance of **risk** (2.61) is evaluated

[ISO Guide 73:2009]

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

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

2.67
risk evaluation
process (2.54) of comparing the results of **risk analysis** (2.63) with **risk criteria** (2.66) to determine whether the **risk** (2.61) and/or its magnitude is acceptable or tolerable

[ISO Guide 73:2009]

NOTE Risk evaluation assists in the decision about risk treatment.

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

[ISO Guide 73:2009]

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

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

2.69
risk management
coordinated activities to direct and control an organisation with regard to **risk** (2.61)

[ISO Guide 73:2009]

2.70
risk management process
systematic application of management **policies** (2.51), **procedures** (2.53) and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing **risk** (2.61)

[ISO Guide 73:2009]

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

2.71
risk treatment
process (2.54) to modify **risk** (2.61)

[ISO Guide 73:2009]

NOTE 1 Risk treatment can involve:

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

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

NOTE 3 Risk treatment can create new risks or modify existing risks.

2.72
scale
ordered set of values, continuous or discrete, or a set of categories to which the **attribute** (2.6) is mapped

[ISO/IEC 15939:2007]

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

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

These are just examples of the types of scale.

2.73
security implementation standard
document specifying authorized ways for realizing security

2.74
stakeholder
person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[ISO Guide 73:2009]

2.75
statement of applicability
documented statement describing the **control objectives** (2.17) and **controls** (2.16) that are relevant and applicable to the organisation's **ISMS** (2.34)

2.76
third party
person or body that is recognized as being independent of the parties involved, as concerns the issue in question

[ISO/IEC 27002:2005]

2.77
threat
potential cause of an unwanted incident, which may result in harm to a system or organisation

2.78
unit of measurement
particular quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitude relative to that quantity

[ISO/IEC 15939:2007]

2.79
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[ISO 9000:2005]

2.80
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2005]

NOTE This could also be called compliance testing.

2.81
vulnerability
weakness of an **asset** (2.4) or **control** (2.16) that can be exploited by one or more **threats** (2.77)

3 Information security management systems

3.1 Introduction

Organisations of all types and sizes:

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

b) recognise that information, and related processes, systems, networks and people are important assets for achieving organisation 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 organisation 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 organisation 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, organisations 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 organisation 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 organisation, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving organisation's information security to achieve business objectives. It is based upon a risk assessment and the organisation'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 organisation'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 organisations information is dependent upon information and communications technology. This technology is often an essential element in the organisation 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, organisational 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 organisation are met. Relevant information security controls are expected to be seamlessly integrated with an organisation's business processes.

3.2.4 Management

Management involves activities to direct, control and continually improve the organisation 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 organisation to management hierarchies consisting of many individuals in large organisations.

In terms of an ISMS, management involves the supervision and making of decisions necessary to achieve business objectives through the protection of the organisation'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 organisation by all individuals associated with the organisation.

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

3.2.5 Management system

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

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

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

b) improve an organisation's plans and activities;

c) meet the organisation'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 organisational goals.

3.3 Process approach

Organisations 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 organisation, together with the identification and interactions of these processes, and their management, can be referred to as a “process approach”.

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

a) Plan – establish objectives and make plans (analyze the organisation's situation, establish the overall objectives and set targets, and develop plans to achieve them);

b) Do – implement plans (do what was planned to do);

c) Check – measure results (measure/monitor the extent to which achievements meet planned objectives); and

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

3.4 Why an ISMS is important

Risks associated with an organisation'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 organisation.

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

The design and implementation of an organisation's ISMS is influenced by the needs and objectives of the organisation, security requirements, the business processes employed and the size and structure of the organisation. The design and operation of an ISMS needs to reflect the interests and information security requirements of all of the organisation'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. Organisations 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 organisations adopt the ISMS family of standards the ability to apply consistent and mutually-recognisable information security principles can be demonstrated to business partners and other interested parties.

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

The successful adoption of an ISMS is important to protect information assets allowing an organisation 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 organisation 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 organisation's information assets (see 3.5.6).

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

3.5.2 Identifying information security requirements

Within the overall strategy and business objectives of the organisation, 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 organisation's information assets will involve analyzing: threats to information assets; vulnerabilities to and the likelihood of a threat materializing to information assets; and the potential impact of any information security incident on information assets. The expenditure on relevant controls is expected to be proportionate to the perceived business impact of the risk materialising.

3.5.3 Assessing information security risks

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

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organisation. 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 organisation 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 organisation. 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 organisation’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 apply for risk reduction.

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

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

b) organisational objectives;

c) operational requirements and constraints;

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

e) 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 27002:2005 are acknowledged as best practices applicable to most organisations and readily tailored to accommodate organisations 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 organisation. 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 organisations.

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 organisation'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 organisation needs to maintain and improve the ISMS through monitoring and assessing performance against organisational 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.

3.6 ISMS critical success factors

A large number of factors are critical to the successful implementation of an ISMS to allow an organisation 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 organisational 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 organisation will consistently achieve the critical success factors required to protect its information assets.

3.7 Benefits of the ISMS family of standards

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

a) a structured manner supporting the process of specifying, implementing, operating and maintaining a comprehensive, cost-effective, value creating, integrated and aligned ISMS that meets the organisation'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 organisations 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 organisation;

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[2)] are illustrated in Figure 1.

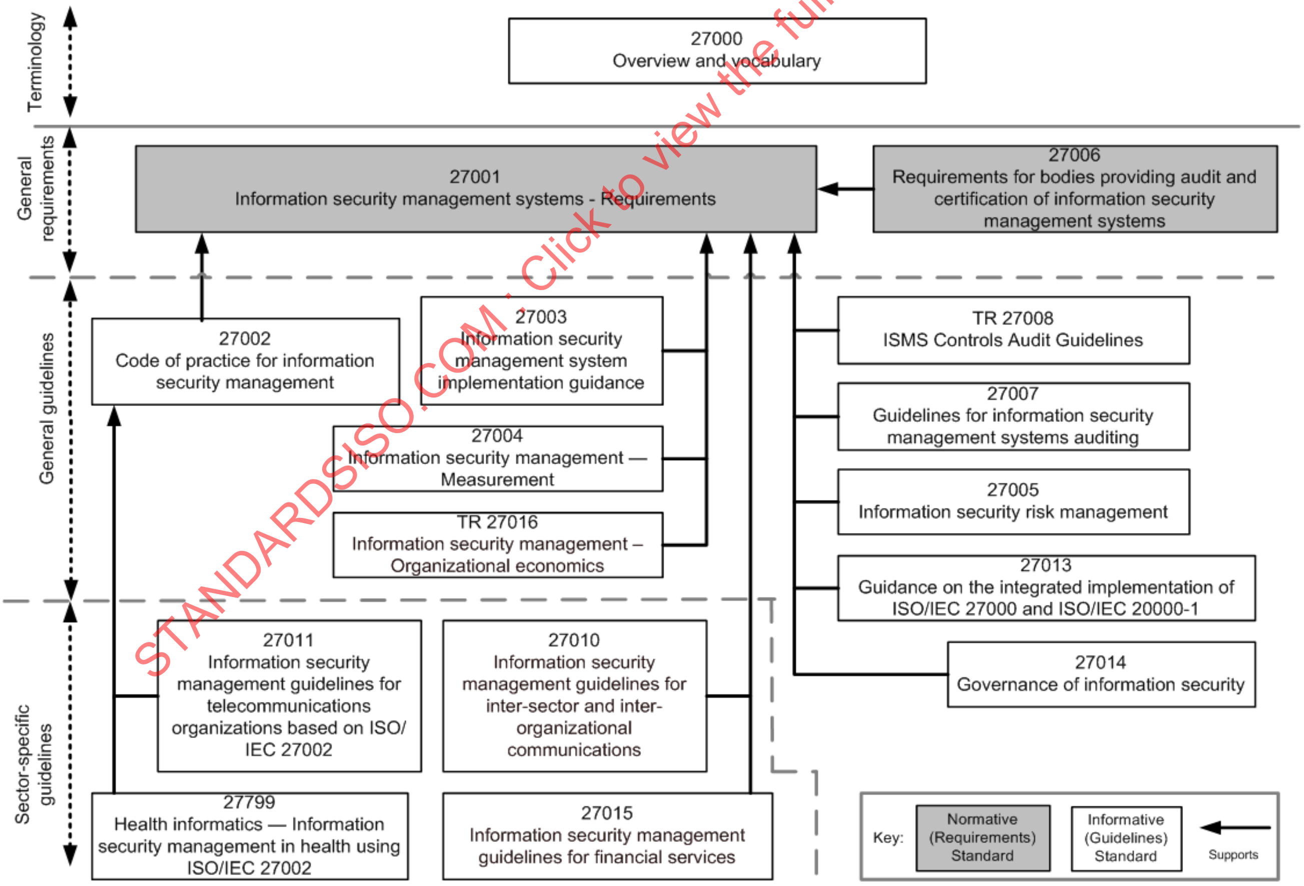
Terminology
General requirements
General guidelines
Sector-specific guidelines
27000 Overview and vocabulary
27001 Information security management systems - Requirements
27006 Requirements for bodies providing audit and certification of information security management systems
27002 Code of practice for information security management
27003 Information security management system implementation guidance
27004 Information security management — Measurement
TR 27016 Information security management – Organizational economics
TR 27008 ISMS Controls Audit Guidelines
27007 Guidelines for information security management systems auditing
27005 Information security risk management
27013 Guidance on the integrated implementation of ISO/IEC 27000 and ISO/IEC 20000-1
27014 Governance of information security
27011 Information security management guidelines for telecommunications organizations based on ISO/ IEC 27002
27010 Information security management guidelines for inter-sector and inter-organizational communications
27799 Health informatics — Information security management in health using ISO/IEC 27002
27015 Information security management guidelines for financial services
Key:
Normative (Requirements) Standard
Informative (Guidelines) Standard
Supports

Figure 1 — ISMS Family of Standards Relationships

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

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

Standard that provides direct support, detailed guidance and/or interpretation for the controls specified in ISO/IEC 27002 (see 4.4.1) is ISO/IEC 27008 (see 4.4.6).

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

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

The ISMS family of standards maintains relationships with many other ISO and ISO/IEC standards and are classified and further described as being either:

a) standards describing an overview and terminology (see 4.2);

b) standards specifying requirements (see 4.3);

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

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

4.2 Standards describing an overview and terminology

4.2.1 ISO/IEC 27000 (this document)

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

Scope: This International Standard provides to organisations 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 organisation's overall business risks. It specifies requirements for the implementation of information security controls customized to the needs of individual organisations or parts thereof. This International Standard can be used by all organisations, regardless of type, size and nature.

[3)] ISO/IEC 27009 is reserved for future standards associated with the ISMS family of standards that have not yet been defined when this International Standard was published.