INTERNATIONAL STANDARD

ISO/IEC 27000

First edition
2009-05-01

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

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité des informations — Vue d'ensemble et vocabulaire

Reference number
ISO/IEC 27000:2009(E)

© ISO/IEC 2009

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2009 – All rights reserved

Contents

Page

Foreword ... iv

0 Introduction ... v

1 Scope ... 1

2 Terms and definitions ... 1

3 Information security management systems ... 6
3.1 Introduction ... 6
3.2 What is an ISMS? ... 7
3.3 Process approach ... 8
3.4 Why an ISMS is important ... 9
3.5 Establishing, monitoring, maintaining and improving an ISMS ... 10
3.6 ISMS critical success factors ... 11
3.7 Benefits of the ISMS family of standards ... 11

4 ISMS family of standards ... 12
4.1 General information ... 12
4.2 Standards describing an overview and terminology ... 13
4.3 Standards specifying requirements ... 13
4.4 Standards describing general guidelines ... 14
4.5 Standards describing sector-specific guidelines ... 15

Annex A (informative) **Verbal forms for the expression of provisions** ... 16

Annex B (informative) **Categorized terms** ... 17

Bibliography ... 19

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

0 Introduction

0.1 Overview

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

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

0.2 ISMS family of standards

The ISMS family of standards[1)] is intended to assist organizations of all types and sizes to implement and operate an ISMS. The ISMS family of standards consists of the following International Standards, under the general title *Information technology — Security techniques*:

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

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

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

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

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

— ISO/IEC 27005:2008, *Information security risk management*

— ISO/IEC 27006:2007, *Requirements for bodies providing audit and certification of information security management systems*

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

— ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

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*

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2009 All rights reserved
Not for Resale

0.3 Purpose of this International Standard

This International Standard provides an overview of information security management systems, which form the subject of the ISMS family of standards, 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 terms for own use.

Standards addressing only the implementation of controls, as opposed to addressing all controls, from ISO/IEC 27002 are excluded from the ISMS family of standards.

To reflect the changing status of the ISMS family of standards, this International Standard is expected to be continually updated on a more frequent basis than would normally be the case for other ISO/IEC standards.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

1 Scope

This International Standard provides:

a) an overview of the ISMS family of standards;

b) an introduction to information security management systems (ISMS);

c) a brief description of the Plan-Do-Check-Act (PDCA) process; and

d) terms and definitions for use in the ISMS family of standards.

This International Standard is applicable to all types of organization (e.g. commercial enterprises, government agencies, non-profit organizations).

2 Terms and definitions

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

NOTE 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 “anything that has value to the organization”.

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

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

2.1
access control
means to ensure that access to **assets** (2.3) is authorized and restricted based on business and security requirements

2.2
accountability
responsibility of an entity for its actions and decisions

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

2.3
asset
anything that has value to the organization

NOTE There are many types of assets, including:

a) **information** (2.18);

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.

2.4
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an **asset** (2.3)

2.5
authentication
provision of assurance that a claimed characteristic of an entity is correct

2.6
authenticity
property that an entity is what it claims to be

2.7
availability
property of being accessible and usable upon demand by an authorized entity

2.8
business continuity
processes (2.31) and/or **procedures** (2.30) for ensuring continued business operations

2.9
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or **processes** (2.31)

2.10
control
means of managing **risk** (2.34), including **policies** (2.28), **procedures** (2.30), **guidelines** (2.16), practices or organizational structures, which can be administrative, technical, management, or legal in nature

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

2.11
control objective
statement describing what is to be achieved as a result of implementing **controls** (2.10)

2.12
corrective action
action to eliminate the cause of a detected nonconformity or other undesirable situation

[ISO 9000:2005]

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.13
effectiveness
extent to which planned activities are realized and planned results achieved

[ISO 9000:2005]

2.14
efficiency
relationship between the results achieved and how well the resources have been used

2.15
event
occurrence of a particular set of circumstances

[ISO/IEC Guide 73:2002]

2.16
guideline
recommendation of what is expected to be done to achieve an objective

2.17
impact
adverse change to the level of business objectives achieved

2.18
information asset
knowledge or data that has value to the organization

2.19
information security
preservation of **confidentiality** (2.9), **integrity** (2.25) and **availability** (2.7) of information

NOTE In addition, other properties, such as **authenticity** (2.6), **accountability** (2.2), **non-repudiation** (2.27), and **reliability** (2.33) can also be involved.

2.20
information security event
identified occurrence of a system, service or network state indicating a possible breach of **information security** (2.19) **policy** (2.28) or failure of **controls** (2.10), or a previously unknown situation that may be security relevant

2.21
information security incident
single or a series of unwanted or unexpected **information security events** (2.20) that have a significant probability of compromising business operations and threatening **information security** (2.19)

2.22
information security incident management
processes (2.31) for detecting, reporting, assessing, responding to, dealing with, and learning from **information security incidents** (2.21)

2.23
information security management system
ISMS
part of the overall **management system** (2.26), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve **information security** (2.19)

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2009 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.24
information security risk
potential that a **threat** (2.45) will exploit a **vulnerability** (2.46) of an **asset** (2.3) or group of assets and thereby cause harm to the organization

2.25
integrity
property of protecting the accuracy and completeness of **assets** (2.3)

2.26
management system
framework of **policies** (2.28), **procedures** (2.30), **guidelines** (2.16) and associated resources to achieve the objectives of the organization

2.27
non-repudiation
ability to prove the occurrence of a claimed **event** (2.15) or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the **event** (2.15) or action and involvement of entities in the **event** (2.15)

2.28
policy
overall intention and direction as formally expressed by management

2.29
preventive action
action to eliminate the cause of a potential nonconformity or other undesirable potential situation

[ISO 9000:2005]

2.30
procedure
specified way to carry out an activity or a **process** (2.31)

[ISO 9000:2005]

2.31
process
set of interrelated or interacting activities which transforms inputs into outputs

[ISO 9000:2005]

2.32
record
document stating results achieved or providing evidence of activities performed

[ISO 9000:2005]

2.33
reliability
property of consistent intended behaviour and results

2.34
risk
combination of the probability of an **event** (2.15) and its consequence

[ISO/IEC Guide 73:2002]

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.35
risk acceptance
decision to accept a **risk** (2.34)

[ISO/IEC Guide 73:2002]

2.36
risk analysis
systematic use of information to identify sources and to estimate **risk** (2.34)

[ISO/IEC Guide 73:2002]

NOTE Risk analysis provides a basis for **risk evaluation** (2.41), **risk treatment** (2.43) and **risk acceptance** (2.35).

2.37
risk assessment
overall **process** (2.31) of **risk analysis** (2.36) and **risk evaluation** (2.41)

[ISO/IEC Guide 73:2002]

2.38
risk communication
exchange or sharing of information about **risk** (2.34) between the decision-maker and other stakeholders

[ISO/IEC Guide 73:2002]

2.39
risk criteria
terms of reference by which the significance of **risk** (2.34) is assessed

[ISO/IEC Guide 73:2002]

2.40
risk estimation
activity to assign values to the probability and consequences of a **risk** (2.34)

[ISO/IEC Guide 73:2002]

2.41
risk evaluation
process (2.31) of comparing the estimated **risk** (2.34) against given **risk criteria** (2.39) to determine the significance of the **risk** (2.34)

[ISO/IEC Guide 73:2002]

2.42
risk management
coordinated activities to direct and control an organization with regard to **risk** (2.34)

[ISO/IEC Guide 73:2002]

NOTE Risk management generally includes **risk assessment** (2.37), **risk treatment** (2.43), **risk acceptance** (2.35), **risk communication** (2.38), risk monitoring and risk review.

2.43
risk treatment
process (2.31) of selection and implementation of measures to modify **risk** (2.34)

[ISO/IEC Guide 73:2002]

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.44
statement of applicability
documented statement describing the **control objectives** (2.11) and **controls** (2.10) that are relevant and applicable to the organization's **ISMS** (2.23)

2.45
threat
potential cause of an unwanted incident, which may result in harm to a system or organization

2.46
vulnerability
weakness of an **asset** (2.3) or **control** (2.10) that can be exploited by a **threat** (2.45)

3 Information security management systems

3.1 Introduction

Organizations of all types and sizes:

a) collect, process, store, and transmit large amounts of information;

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

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

d) modify risks 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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.2 What is an ISMS?

3.2.1 Overview and principles

An ISMS (Information Security Management System) provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve business objectives based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:

a) awareness of the need for information security;

b) assignment of responsibility for information security;

c) incorporating management commitment and the interests of stakeholders;

d) enhancing societal values;

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

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

g) active prevention and detection of information security incidents;

h) ensuring a comprehensive approach to information security management; and

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

3.2.2 Information

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

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

3.2.3 Information security

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

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 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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.2.4 Management

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

In terms of an ISMS, management involves the supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets. Management of information security is expressed through the formulation and use of information security policies, standards, procedures and guidelines, which are then applied throughout the organization by all individuals associated with the organization.

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

3.2.5 Management system

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

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

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

b) improve an organization's plans and activities;

c) meet the organization's information security objectives;

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

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

3.3 Process approach

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

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

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

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

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

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

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.4 Why an ISMS is important

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

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

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

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

An ISMS is important to both public and private sector businesses. In any industry, an ISMS is an enabler that supports e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increases the difficulty of controlling access to and handling of information. In addition, the distribution of mobile storage devices containing information assets can weaken the effectiveness of traditional controls. When organizations adopt the ISMS family of standards the ability to apply consistent and mutually-recognisable information security principles can be demonstrated to business partners and other interested parties.

Information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the 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 security requirements.

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

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

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

c) continually improve its control environment; and

d) effectively achieve legal and regulatory compliance.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.5 Establishing, monitoring, maintaining and improving an ISMS

3.5.1 Overview

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

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

b) assess information security risks (see 3.5.3);

c) select and implement relevant controls to manage unacceptable risks (see 3.5.4); and

d) monitor, maintain and improve the effectiveness of security controls associated with the organization's information assets (see 3.5.5).

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

3.5.2 Identify information security requirements

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

a) identified information assets and their value;

b) business needs for information processing and storage; and

c) legal, regulatory, and contractual requirements.

Conducting a methodical assessment of the risks associated with the organization's information assets will involve analyzing: threats to information assets; vulnerabilities to and the likelihood of a threat materializing to information assets; and the potential impact of any information security incident on information assets. The expenditure on relevant security controls is expected to be proportionate to the perceived business impact of the risk materialising.

3.5.3 Assess 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, social, economical and environmental aspects, the concerns of stakeholders, priorities, and other inputs and variables as appropriate. The results of the information security risk assessment will help to guide and determine the appropriate management treatment decisions for action and prioritisation for managing information security risks, and for implementing relevant security controls to protect against these risks. ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

3.5.4 Select and implement information security controls

Once information security requirements have been identified and information security risks to the identified information assets have been determined and assessed (including decisions for the treatment of information security risks having been made), appropriate controls need to be selected and implemented to ensure that information security risks are reduced to a level acceptable to the organization. Controls may be selected from ISO/IEC 27002, from other relevant control sets, or new controls designed to meet specific needs as appropriate. The selection of security controls is dependent upon security requirements taking into account the criteria for information security risk acceptance, risk treatment options, and the general risk management approach applied by the organization. The selection and implementation of controls may be documented within a statement of applicability to assist with compliance requirements.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 information security controls for the management system (ISO/IEC 27001).

3.5.5 Monitor, maintain and improve the effectiveness of the ISMS

An organization needs to maintain and improve the ISMS through monitoring and assessing performance against organization policy and objectives, and reporting the results to management for review. This ISMS review will allow evidence of validation, verification, and traceability of corrective, preventive and improvement actions based on the records of these monitored areas, including the monitoring of information security controls.

3.6 ISMS critical success factors

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

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

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

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

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

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

f) an effective information security incident management process;

g) an effective business continuity management approach; and

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

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

3.7 Benefits of the ISMS family of standards

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

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

b) assistance for management in structuring 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;

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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; and

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.

4 ISMS family of standards

4.1 General information

The ISMS family of standards consists of inter-related standards, either already published or under development, and contains a number of significant structural components. These components are focused upon normative standards describing ISMS requirements (ISO/IEC 27001) and certification body requirements (ISO/IEC 27006) for those certifying compliance with ISO/IEC 27001. Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process, control-related guidelines as well as sector-specific guidance. Relationships between the ISMS family of standards[2)] are illustrated in Figure 1.

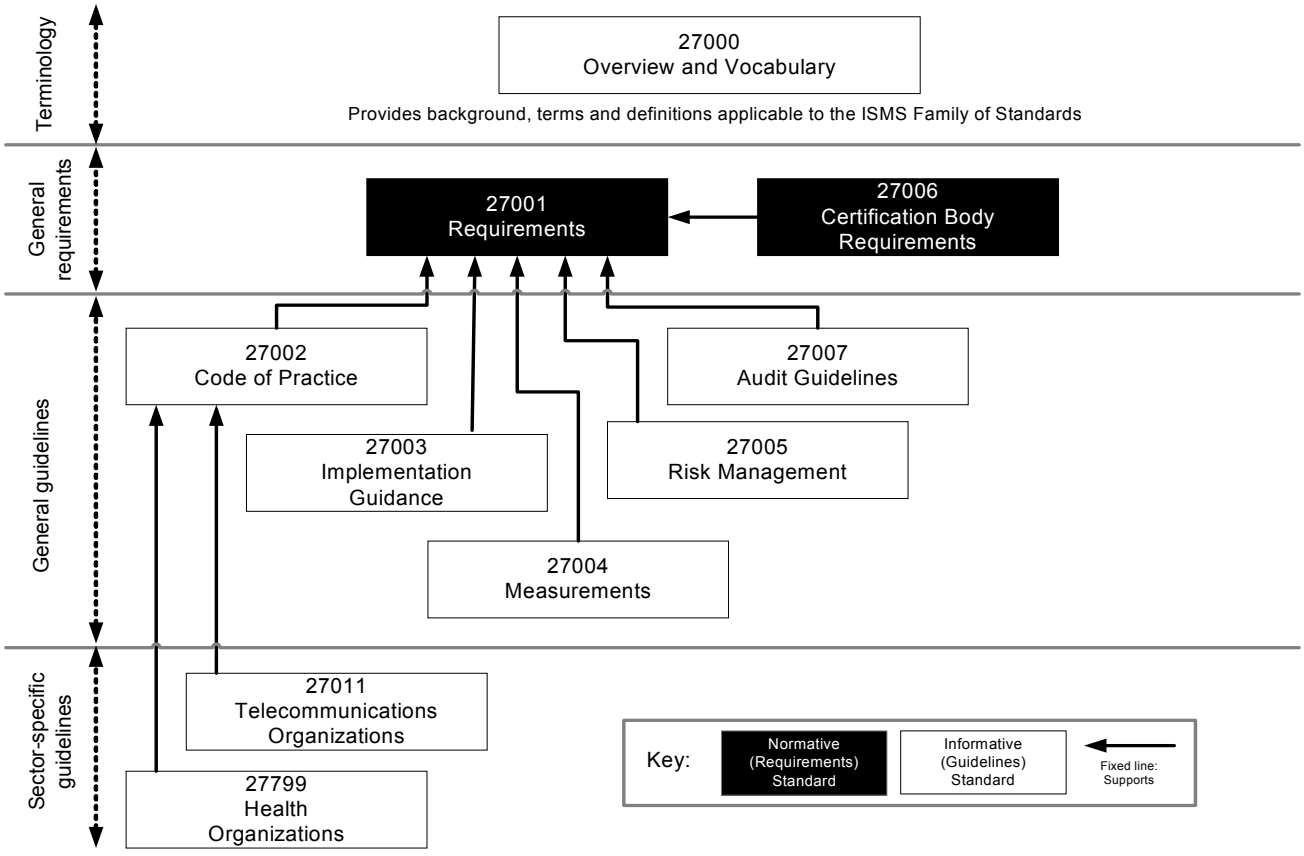

Figure 1 — ISMS Family of Standards Relationships

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) and ISO/IEC 27007 (see 4.4.5).

2) ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27007 are currently under development.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ISO/IEC 27006 (see 4.3.2) addresses requirements of bodies providing ISMS certifications. ISO/IEC 27011 (see 4.5.1) and ISO 27799 (4.5.2) addresses 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 organizations and individuals:

a) an overview of the ISMS family of standards;

b) an introduction to information security management systems (ISMS);

c) a brief description of the Plan-Do-Check-Act (PDCA) process; and

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

Purpose: ISO/IEC 27000 describes the fundamentals of information security management systems, which form the subject of the ISMS family of standards, and defines related terms.

4.3 Standards specifying requirements

4.3.1 ISO/IEC 27001

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

Scope: This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. This International Standard is universal for all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations).

Purpose: ISO/IEC 27001 provides normative requirements for the development and operation of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. Organizations operating an ISMS may have its conformity audited and certified. The control objectives and controls from Annex A (ISO/IEC 27001) shall be selected as part of this ISMS process as appropriate to cover the identified requirements. The control objectives and controls listed in Table A.1 (ISO/IEC 27001) are directly derived from and aligned with those listed in ISO/IEC 27002 Clauses 5 to 15.

3) ISO/IEC 27008, ISO/IEC 27009 and ISO/IEC 27010 are reserved for future standards associated with the ISMS family of standards that have not yet been defined when this International Standard was published.

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.3.2 ISO/IEC 27006

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

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

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

4.4 Standards describing general guidelines

4.4.1 ISO/IEC 27002

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

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

Purpose: ISO/IEC 27002 provides guidance on the implementation of information security controls. Specifically Clauses 5 to 15 provides specific implementation advice and guidance on best practice in support of the controls specified in Clauses A.5 to A.15 of ISO/IEC 27001.

4.4.2 ISO/IEC 27003

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

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

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

4.4.3 ISO/IEC 27004

Information technology — Security techniques — Information security management — Measurement

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

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.4.4 ISO/IEC 27005

Information technology — Security techniques — Information security risk management

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

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

4.4.5 ISO/IEC 27007

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

Scope: This International Standard will provide 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 managements systems in general.

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

4.5 Standards describing sector-specific guidelines

4.5.1 ISO/IEC 27011

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

Scope: This International Standard provides guidelines supporting the implementation of Information Security Management (ISM) in telecommunications organizations.

Purpose: ISO/IEC 27011 provides telecommunications organisations with an adaptation of the ISO/IEC 27002 guidelines unique to their industry sector which are additional to the guidance provided towards fulfilling the requirements of ISO/IEC 27001, Annex A.

4.5.2 ISO 27799

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

Scope: This International Standard provides guidelines supporting the implementation of Information Security Management (ISM) in health organizations.

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

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(informative)

Verbal forms for the expression of provisions

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

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

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

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(informative)

Categorized terms

B.1 Terms relating to information security

2.2 accountability

2.5 authentication

2.6 authenticity

2.7 availability

2.9 confidentiality

2.19 information security

2.25 integrity

2.27 non-repudiation

2.33 reliability

B.2 Terms relating to management

2.8 business continuity

2.12 corrective action

2.13 effectiveness

2.14 efficiency

2.16 guideline

2.23 information security management system (ISMS)

2.26 management system

2.28 policy

2.29 preventive action

2.31 process

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.3 Terms relating to information security risk

2.1 access control

2.3 asset

2.4 attack

2.10 control

2.11 control objective

2.15 event

2.17 impact

2.18 information asset

2.20 information security event

2.21 information security incident

2.22 information security incident management

2.24 information security risk

2.34 risk

2.35 risk acceptance

2.36 risk analysis

2.37 risk assessment

2.38 risk communication

2.39 risk criteria

2.40 risk estimation

2.41 risk evaluation

2.42 risk management

2.43 risk treatment

2.45 threat

2.46 vulnerability

B.4 Terms relating to documentation

2.30 procedure

2.32 record

2.44 statement of applicability

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] ISO/IEC 17021:2006, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[4] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[6] ISO/IEC 27003[4)], *Information technology — Security techniques — Information security management system implementation guidance*

[7] ISO/IEC 27004[5)], *Information technology — Security techniques — Information security management — Measurement*

[8] ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*

[9] ISO/IEC 27006:2007*, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[10] ISO/IEC 27007[6)]*, Information technology — Security techniques — Guidelines for information security management systems auditing*

[11] ISO/IEC 27011[7)], *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

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

[13] ISO/IEC Guide 73:2002*, Risk Management — Vocabulary — Guidelines for use in standards*

4) To be published.

5) To be published.

6) To be published.

7) To be published.

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 01.040.35; 35.040

Price based on 19 pages

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale