INTERNATIONAL STANDARD

ISO/IEC 27005

Second edition
2011-06-01

Information technology — Security techniques — Information security risk management

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

Reference number
ISO/IEC 27005:2011(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

Contents

Page

Foreword

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

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

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

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

ISO/IEC 27005 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 27005:2008) which has been technically revised.

Introduction

This International Standard provides guidelines for information security risk management in an organization, supporting in particular the requirements of an information security management (ISMS) according to ISO/IEC 27001. However, this International Standard does not provide any specific method for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS.

This International Standard is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.

Information technology — Security techniques — Information security risk management

1 Scope

This International Standard provides guidelines for information security risk management.

This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this International Standard.

This International Standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

NOTE Differences in definitions between ISO/IEC 27005:2008 and this International Standard are shown in Annex G.

3.1
consequence
outcome of an **event** (3.3) 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.

3.2
control
measure that is modifying **risk** (3.9)

[ISO Guide 73:2009]

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

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

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

3.3
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”.

3.4
external context
external environment in which the organization 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 organization; and

— relationships with, and perceptions and values of, external stakeholders.

3.5
internal context
internal environment in which the organization seeks to achieve its objectives

[ISO Guide 73:2009]

NOTE Internal context can include:

— governance, organizational structure, roles and accountabilities;

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

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

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

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

— the organization's culture;

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

— form and extent of contractual relationships.

3.6
level of risk
magnitude of a **risk** (3.9), expressed in terms of the combination of **consequences** (3.1) and their **likelihood** (3.7)

[ISO Guide 73:2009]

3.7
likelihood
chance of something happening

[ISO Guide 73:2009]

NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

3.8
residual risk
risk (3.9) remaining after **risk treatment** (3.17)

[ISO Guide 73:2009]

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as "retained risk".

3.9
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, organization-wide, project, product and process).

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

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

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

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

3.10
risk analysis
process to comprehend the nature of risk and to determine the **level of risk** (3.6)

[ISO Guide 73:2009]