

Redline version
compares Third edition to
Second edition



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*

ITeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/6d253761-0880-4009-9714-bb115a4a4251/iso-iec-27005-2018>





Reference number
ISO/IEC 27005:redline:2018(E)

© ISO/IEC 2018

IMPORTANT — PLEASE NOTE

This is a mark-up copy and uses the following colour coding:

- | | |
|---|---|
| Text example 1 | — indicates added text (in green) |
| Text example 2 | — indicates removed text (in red) |
|  | — indicates added graphic figure |
|  | — indicates removed graphic figure |
| 1.x ... | — Heading numbers containg modifications are highlighted in yellow in the Table of Contents |

DISCLAIMER

This Redline version provides you with a quick and easy way to compare the main changes between this edition of the standard and its previous edition. It doesn't capture all single changes such as punctuation but highlights the modifications providing customers with the most valuable information. Therefore it is important to note that this Redline version is not the official ISO standard and that the users must consult with the clean version of the standard, which is the official standard, for implementation purposes.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure of this International Standard document	5
5 Background	6
6 Overview of the information security risk management process	7
7 Context establishment	11
7.1 General considerations	11
7.2 Basic criteria	11
7.2.1 Risk management approach	11
7.2.2 Risk evaluation criteria	12
7.2.3 Impact criteria	12
7.2.4 Risk acceptance criteria	12
7.3 Scope and boundaries	13
7.4 Organization for information security risk management	14
8 Information security risk assessment	14
8.1 General description of information security risk assessment	14
8.2 Risk identification	15
8.2.1 Introduction to risk identification	15
8.2.2 Identification of assets	15
8.2.3 Identification of threats	16
8.2.4 Identification of existing controls	16
8.2.5 Identification of vulnerabilities	17
8.2.6 Identification of consequences	18
8.3 Risk analysis	18
8.3.1 Risk analysis methodologies	18
8.3.2 Assessment of consequences	20
8.3.3 Assessment of incident likelihood	21
8.3.4 Level of risk determination	21
8.4 Risk evaluation	22
9 Information security risk treatment	23
9.1 General description of risk treatment	23
9.2 Risk modification	25
9.3 Risk retention	26
9.4 Risk avoidance	26
9.5 Risk sharing	26
10 Information security risk acceptance	27
11 Information security risk communication and consultation	27
12 Information security risk monitoring and review	28
12.1 Monitoring and review of risk factors	28
12.2 Risk management monitoring, review and improvement	29
Annex A (informative) Defining the scope and boundaries of the information security risk management process	31
Annex B (informative) Identification and valuation of assets and impact assessment	37
Annex C (informative) Examples of typical threats	53

Annex D (informative) Vulnerabilities and methods for vulnerability assessment	58
Annex E (informative) Information security risk assessment approaches	64
Annex F (informative) Constraints for risk modification	71
Annex G (informative) Differences in definitions between ISO/IEC 27005:2008 and ISO/IEC 27005:2011	75
Bibliography	84

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/6d253761-0bcc-4009-9714-bb115a4a4251/iso-iec-27005-2018>

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

~~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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

~~ISO/IEC 27005~~ This document was prepared by ~~Joint~~ Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This ~~second~~ ~~third~~ edition cancels and replaces the ~~first~~ ~~second~~ edition (ISO/IEC 27005:2008/2011) which has been technically revised. The main changes from the previous edition are as follows:

- all direct references to the ISO/IEC 27001:2005 have been removed;
- clear information has been added that this document does not contain direct guidance on the implementation of the ISMS requirements specified in ISO/IEC 27001 (see Introduction);
- ISO/IEC 27001:2005 has been removed from Clause 2;
- ISO/IEC 27001 has been added to the Bibliography;
- Annex G and all references to it have been removed;
- editorial changes have been made accordingly.

Introduction

This ~~International Standard~~ document 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~~ document 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~~ an information security management system (ISMS), context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this ~~International Standard~~ document to implement the requirements of an ISMS. This document is based on the asset, threat and vulnerability risk identification method that is no longer required by ISO/IEC 27001. There are some other approaches that can be used.

This document does not contain direct guidance on the implementation of the ISMS requirements given in ISO/IEC 27001.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/6d253761-0bcc-4009-9714-bb115a4a4251/iso-iec-27005-2018>

Information technology — Security techniques — Information security risk management

1 Scope

This International Standard document provides guidelines for information security risk management.

This International Standard document 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 document.

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

2 Normative references

The following referenced documents are indispensable for the application of referred to in the text in such a way that some or all of their content constitutes requirements 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~~

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

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~~

~~[SOURCE: ISO Guide 73:2009]~~

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

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

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

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

~~3.2~~

~~control~~

~~measure that is modifying risk (3.9)~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. 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 to entry. Controls may not always exert the intended or assumed modifying effect.~~

~~Note 3 to entry. Control is also used as a synonym for safeguard or countermeasure.~~

~~3.3~~

~~event~~

~~occurrence or change of a particular set of circumstances~~

~~[SOURCE: ISO Guide 73:2009]~~

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

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

~~Note 3 to entry. An event can sometimes be referred to as an "incident" or "accident".~~

~~3.4~~

~~external context~~

~~external environment in which the organization seeks to achieve its objectives~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. External context can include:~~

- ~~— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;~~
- ~~— key drivers and trends having impact on the objectives 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~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. Internal context can include:~~

- ~~— governance, organizational structure, roles and accountabilities,~~
- ~~— policies, objectives, and the strategies that are in place to achieve them,~~
- ~~— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies),~~
- ~~— information systems, information flows and decision-making processes (both formal and informal),~~
- ~~— relationships with, and perceptions and values of, internal stakeholders,~~
- ~~— the organization's culture,~~
- ~~— standards, guidelines and models adopted by the organization, and~~
- ~~— form and extent of contractual relationships.~~

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)~~

~~[SOURCE: ISO Guide 73:2009]~~

3.7**likelihood**

~~chance of something happening~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. 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 to entry. 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)~~

~~[SOURCE: ISO Guide 73:2009]~~

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

~~Note 2 to entry. Residual risk can also be known as “retained risk”.~~

3.9**risk**

~~effect of uncertainty on objectives~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. An effect is a deviation from the expected — positive and/or negative.~~

~~Note 2 to entry. 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 to entry. Risk is often characterized by reference to potential events (3.3) and consequences (3.1), or a combination of these.~~

~~Note 4 to entry. 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 to entry. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.~~

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

3.10**risk analysis**

~~process to comprehend the nature of risk and to determine the level of risk (3.6)~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. Risk analysis provides the basis for risk evaluation and decisions about risk treatment.~~

~~Note 2 to entry. Risk analysis includes risk estimation.~~

~~3.11~~

~~risk assessment~~

~~overall process of risk identification (3.15), risk analysis (3.10) and risk evaluation (3.14)~~

~~[SOURCE: ISO Guide 73:2009]~~

~~3.12~~

~~risk communication and consultation~~

~~continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders (3.10) regarding the management of risk (3.2)~~

~~[SOURCE: ISO Guide 73:2009]~~

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

~~Note 2 to entry. Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:~~

~~— a process which impacts on a decision through influence rather than power, and~~

~~— an input to decision making, not joint decision making.~~

~~3.13~~

~~risk criteria~~

~~terms of reference against which the significance of a risk (3.2) is evaluated~~

~~[SOURCE: ISO Guide 73:2009]~~

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

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

~~3.14~~

~~risk evaluation~~

~~process of comparing the results of risk analysis (3.10) with risk criteria (3.13) to determine whether the risk and/or its magnitude is acceptable or tolerable~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. Risk evaluation assists in the decision about risk treatment.~~

~~3.15~~

~~risk identification~~

~~process of finding, recognizing and describing risks~~

~~[SOURCE: ISO Guide 73:2009]~~

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

~~Note 2 to entry. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.~~

~~3.16~~

~~risk management~~

~~coordinated activities to direct and control an organization with regard to risk~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. This International Standard uses the term 'process' to describe risk management overall. The elements within the risk management process are termed 'activities'.~~

3.17**risk treatment**

~~process to modify risk~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. Risk treatment can involve:~~

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

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

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

3.18**stakeholder**

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

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry. decision maker can be a stakeholder.~~

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

4 Structure of this International Standard document

This International Standard document contains the description of the information security risk management process and its activities.

The background information is provided in [Clause 5](#).

A general overview of the information security risk management process is given in [Clause 6](#).

All information security risk management activities as presented in [Clause 6](#) are subsequently described in the following clauses:

- context establishment in [Clause 7](#);
- risk assessment in [Clause 8](#);
- risk treatment in [Clause 9](#);
- risk acceptance in [Clause 10](#);
- risk communication in [Clause 11](#);
- risk monitoring and review in [Clause 12](#).

Additional information for information security risk management activities is presented in the annexes. The context establishment is supported by [Annex A](#) (Defining the scope and boundaries of the information security risk management process). Identification and valuation of assets and impact assessments are discussed in [Annex B](#). [Annex C](#) gives examples of typical threats and [Annex D](#) discusses vulnerabilities and methods for vulnerability assessment. Examples of information security risk assessment approaches are presented in [Annex E](#).

Constraints for risk modification are presented in [Annex F](#).

~~Differences in definitions between ISO/IEC 27005:2008 and ISO/IEC 27005:2011 are shown in [Annex G](#).~~

All risk management activities as presented from [Clause 7](#) to [Clause 12](#) are structured as follows:

Input: Identifies any required information to perform the activity.

Action: Describes the activity.

Implementation guidance: Provides guidance on performing the action. Some of this guidance may not be suitable in all cases and so other ways of performing the action may be more appropriate.

Output: Identifies any information derived after performing the activity.

5 Background

A systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS). This approach should be suitable for the organization's environment, and in particular organization's environment and, in particular, should be aligned with overall enterprise risk management. Security efforts should address risks in an effective and timely manner where and when they are needed. Information security risk management should be an integral part of all information security management activities and should be applied both to the implementation and the ongoing operation of an ISMS.

Information security risk management should be a continual process. The process should establish the external and internal context, assess the risks and treat the risks using a risk treatment plan to implement the recommendations and decisions. Risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce the risk to an acceptable level.

Information security risk management should contribute to the following:

- risks being identified;
- risks being assessed in terms of their consequences to the business and the likelihood of their occurrence;
- the likelihood and consequences of these risks being communicated and understood;
- priority order for risk treatment being established;
- priority for actions to reduce risks occurring;
- stakeholders being involved when risk management decisions are made and kept informed of the risk management status;
- effectiveness of risk treatment monitoring;
- risks and the risk management process being monitored and reviewed regularly;
- information being captured to improve the risk management approach;
- managers and staff being educated about the risks and the actions taken to mitigate them;

The information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

6 Overview of the information security risk management process

A high level view of the risk management process is specified in ISO 31000 and shown in [Figure 1](#).

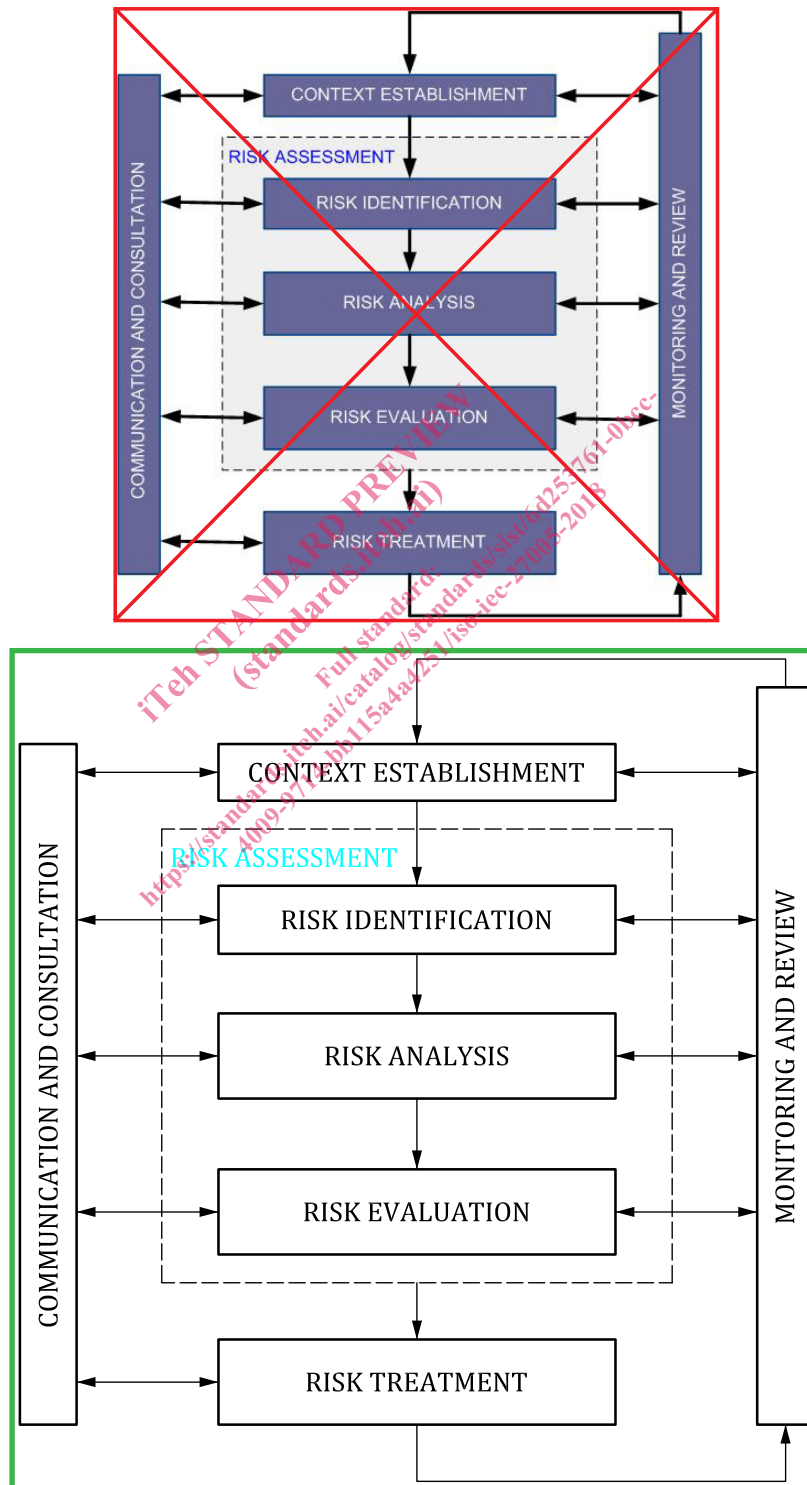


Figure 1 — The risk management process