



SLOVENSKI STANDARD SIST ISO/IEC 27005:2011

01-september-2011

Informacijska tehnologija - Varnostne tehnike- Obvladovanje informacijskih varnostnih tveganj

Information technology - Security techniques - Information security risk management

Technologies de l'information - Techniques de sécurité - Management du risque de la sécurité de l'information

STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: ISO/IEC 27005:2011

SIST ISO/IEC 27005:2011
<https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011>

ICS:

35.040

Nabori znakov in kodiranje
informacij

Character sets and
information coding

SIST ISO/IEC 27005:2011

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST ISO/IEC 27005:2011](#)

<https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011>

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*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST ISO/IEC 27005:2011](https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011)

[https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-
743a610339e8/sist-iso-iec-27005-2011](https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011)

Reference number
ISO/IEC 27005:2011(E)



iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST ISO/IEC 27005:2011](https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011)

<https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure of this International Standard	5
5 Background.....	6
6 Overview of the information security risk management process	7
7 Context establishment.....	10
7.1 General considerations.....	10
7.2 Basic Criteria	10
7.2.1 Risk management approach	10
7.2.2 Risk evaluation criteria	10
7.2.3 Impact criteria	11
7.2.4 Risk acceptance criteria	11
7.3 Scope and boundaries	12
7.4 Organization for information security risk management	12
8 Information security risk assessment.....	13
8.1 General description of information security risk assessment	13
8.2 Risk identification.....	13
8.2.1 Introduction to risk identification	13
8.2.2 Identification of assets.....	14
8.2.3 Identification of threats.....	14
8.2.4 Identification of existing controls.....	15
8.2.5 Identification of vulnerabilities	15
8.2.6 Identification of consequences.....	16
8.3 Risk analysis.....	17
8.3.1 Risk analysis methodologies	17
8.3.2 Assessment of consequences.....	18
8.3.3 Assessment of incident likelihood	18
8.3.4 Level of risk determination.....	19
8.4 Risk evaluation	19
9 Information security risk treatment.....	20
9.1 General description of risk treatment	20

ISO/IEC 27005:2011(E)

9.2	Risk modification	22
9.3	Risk retention	23
9.4	Risk avoidance	23
9.5	Risk sharing	23
10	Information security risk acceptance	24
11	Information security risk communication and consultation	24
12	Information security risk monitoring and review	25
12.1	Monitoring and review of risk factors	25
12.2	Risk management monitoring, review and improvement	26
Annex A	(informative) Defining the scope and boundaries of the information security risk management process	28
A.1	Study of the organization	28
A.2	List of the constraints affecting the organization	29
A.3	List of the legislative and regulatory references applicable to the organization	31
A.4	List of the constraints affecting the scope	31
Annex B	(informative) Identification and valuation of assets and impact assessment	33
B.1	Examples of asset identification	33
B.1.1	The identification of primary assets	33
B.1.2	List and description of supporting assets	34
B.2	Asset valuation	38
B.3	Impact assessment	41
Annex C	(informative) Examples of typical threats	42
Annex D	(informative) Vulnerabilities and methods for vulnerability assessment	45
D.1	Examples of vulnerabilities	45
D.2	Methods for assessment of technical vulnerabilities	48
Annex E	(informative) Information security risk assessment approaches	50
E.1	High-level information security risk assessment	50
E.2	Detailed information security risk assessment	51
E.2.1	Example 1 Matrix with predefined values	52
E.2.2	Example 2 Ranking of Threats by Measures of Risk	54
E.2.3	Example 3 Assessing a value for the likelihood and the possible consequences of risks	54
Annex F	(informative) Constraints for risk modification	56
Annex G	(informative) Differences in definitions between ISO/IEC 27005:2008 and ISO/IEC 27005:2011	58
	Bibliography	68

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.

[SIST ISO/IEC 27005:2011](https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011)

<https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011>

ISO/IEC 27005:2011(E)**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.

**iTeh STANDARD PREVIEW
(standards.iteh.ai)**

[SIST ISO/IEC 27005:2011](https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011)

<https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011>

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.

iTeh STANDARD PREVIEW

2 Normative references (standards.iteh.ai)

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.

ISO/IEC 27005:2011(E)**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 standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011

- 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”

<https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-743a610339e8/sist-iso-iec-27005-2011>

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]

ISO/IEC 27005:2011(E)

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

NOTE 2 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)

[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** (3.18) regarding the management of **risk** (3.9)

[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 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** (3.9) is evaluated

[ISO Guide 73:2009]

[SIST ISO/IEC 27005:2011](https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842-)

<https://standards.iteh.ai/catalog/standards/sist/e7074976-b45c-4468-b842->

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

NOTE 2 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

[ISO Guide 73:2009]

NOTE Risk evaluation assists in the decision about risk treatment.

3.15**risk identification**

process of finding, recognizing and describing risks

[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.

3.16**risk management**

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

[ISO Guide 73:2009]

NOTE 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

[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.

3.18**stakeholder**

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

[ISO Guide 73:2009]

NOTE A decision maker can be a stakeholder.

4 Structure of this International Standard

This International Standard 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,

ISO/IEC 27005:2011(E)

- 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.

ITeh STANDARD PREVIEW
(standards.iteh.ai)

5 Background

SIST ISO/IEC 27005:2011

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 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.

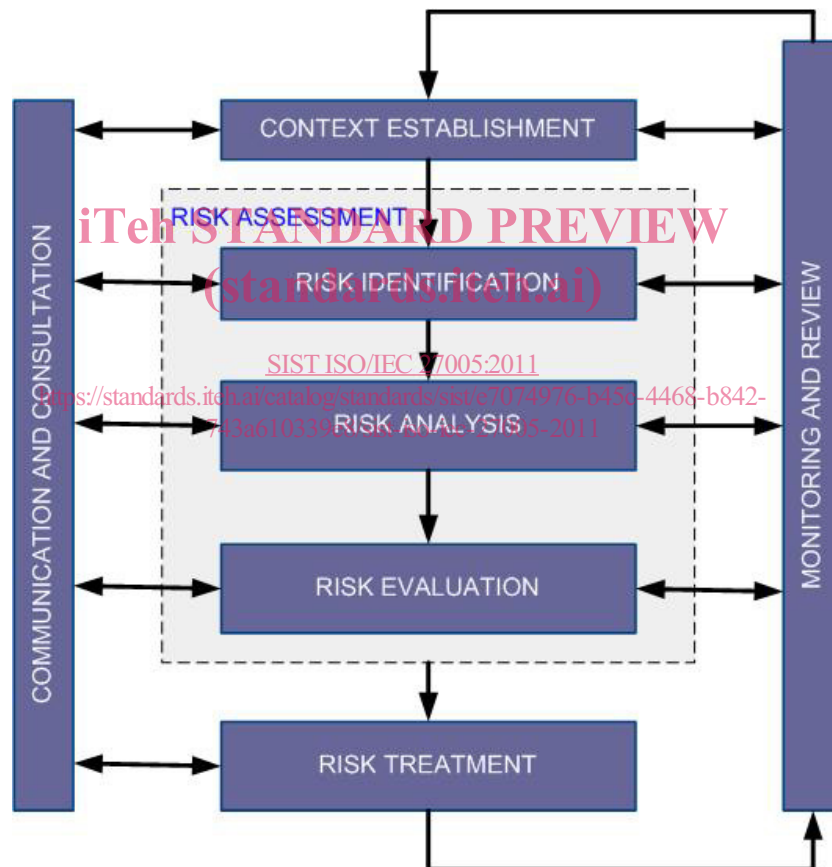


Figure 1 — The risk management process