



SLOVENSKI STANDARD SIST EN ISO/IEC 27005:2024

01-oktober-2024

Informacijska varnost, kibernetika varnost in varovanje zasebnosti - Navodila za obvladovanje informacijskih varnostnih tveganj (ISO/IEC 27005:2022)

Information security, cybersecurity and privacy protection - Guidance on managing information security risks (ISO/IEC 27005:2022)

Informationssicherheit, Cybersicherheit und Datenschutz - Leitfaden zur Handhabung von Informationssicherheitsrisiken (ISO/IEC 27005:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Préconisations pour la gestion des risques liés à la sécurité de l'information (ISO/IEC 27005:2022)

Ta slovenski standard je istoveten z: EN ISO/IEC 27005:2024

[SIST EN ISO/IEC 27005:2024](https://standards.nemur.si/catalog/standards/sist/2024/01/01/27005-2024)

<https://standards.nemur.si/catalog/standards/sist/2024/01/01/27005-2024>

ICS:

03.100.70	Sistemi vodenja	Management systems
35.030	Informacijska varnost	IT Security

SIST EN ISO/IEC 27005:2024

en,fr,de

EUROPEAN STANDARD

EN ISO/IEC 27005

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2024

ICS 35.030

English version

Information security, cybersecurity and privacy protection
- Guidance on managing information security risks
(ISO/IEC 27005:2022)

Sécurité de l'information, cybersécurité et protection
de la vie privée - Préconisations pour la gestion des
risques liés à la sécurité de l'information (ISO/IEC
27005:2022)

Informationssicherheit, Cybersicherheit und
Datenschutz - Leitfaden zur Handhabung von
Informationssicherheitsrisiken (ISO/IEC 27005:2022)

This European Standard was approved by CEN on 1 August 2024.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

EN ISO/IEC 27005:2024 (E)

Contents	Page
European foreword.....	3

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[SIST EN ISO/IEC 27005:2024](https://standards.itih.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024)

<https://standards.itih.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024>

European foreword

The text of ISO/IEC 27005:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27005:2024 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2025, and conflicting national standards shall be withdrawn at the latest by February 2025.

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

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

(<https://standards.iteh.ai>)
Endorsement notice
Document Preview

The text of ISO/IEC 27005:2022 has been approved by CEN-CENELEC as EN ISO/IEC 27005:2024 without any modification.

[SIST EN ISO/IEC 27005:2024](https://standards.iteh.ai/catalog/standards/sist/509c590f-51e7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024)

<https://standards.iteh.ai/catalog/standards/sist/509c590f-51e7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024>

INTERNATIONAL
STANDARD

ISO/IEC
27005

Fourth edition
2022-10

**Information security, cybersecurity
and privacy protection — Guidance on
managing information security risks**

*Sécurité de l'information, cybersécurité et protection de la vie
privée — Préconisations pour la gestion des risques liés à la sécurité
de l'information*

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[SIST EN ISO/IEC 27005:2024](https://standards.iteh.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024)

<https://standards.iteh.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024>



Reference number
ISO/IEC 27005:2022(E)

© ISO/IEC 2022

ISO/IEC 27005:2022(E)

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[SIST EN ISO/IEC 27005:2024](https://standards.iteh.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024)

<https://standards.iteh.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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
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
3.1 Terms related to information security risk.....	1
3.2 Terms related to information security risk management.....	5
4 Structure of this document	7
5 Information security risk management	7
5.1 Information security risk management process.....	7
5.2 Information security risk management cycles.....	9
6 Context establishment	9
6.1 Organizational considerations.....	9
6.2 Identifying basic requirements of interested parties.....	10
6.3 Applying risk assessment.....	10
6.4 Establishing and maintaining information security risk criteria.....	11
6.4.1 General.....	11
6.4.2 Risk acceptance criteria.....	11
6.4.3 Criteria for performing information security risk assessments.....	13
6.5 Choosing an appropriate method.....	15
7 Information security risk assessment process	16
7.1 General.....	16
7.2 Identifying information security risks.....	17
7.2.1 Identifying and describing information security risks.....	17
7.2.2 Identifying risk owners.....	18
7.3 Analysing information security risks.....	19
7.3.1 General.....	19
7.3.2 Assessing potential consequences.....	19
7.3.3 Assessing likelihood.....	20
7.3.4 Determining the levels of risk.....	22
7.4 Evaluating the information security risks.....	22
7.4.1 Comparing the results of risk analysis with the risk criteria.....	22
7.4.2 Prioritizing the analysed risks for risk treatment.....	23
8 Information security risk treatment process	23
8.1 General.....	23
8.2 Selecting appropriate information security risk treatment options.....	23
8.3 Determining all controls that are necessary to implement the information security risk treatment options.....	24
8.4 Comparing the controls determined with those in ISO/IEC 27001:2022, Annex A.....	27
8.5 Producing a Statement of Applicability.....	27
8.6 Information security risk treatment plan.....	28
8.6.1 Formulation of the risk treatment plan.....	28
8.6.2 Approval by risk owners.....	29
8.6.3 Acceptance of the residual information security risks.....	30
9 Operation	31
9.1 Performing information security risk assessment process.....	31
9.2 Performing information security risk treatment process.....	31
10 Leveraging related ISMS processes	32
10.1 Context of the organization.....	32
10.2 Leadership and commitment.....	32

ISO/IEC 27005:2022(E)

10.3	Communication and consultation.....	33
10.4	Documented information.....	35
	10.4.1 General.....	35
	10.4.2 Documented information about processes.....	35
	10.4.3 Documented information about results.....	35
10.5	Monitoring and review.....	36
	10.5.1 General.....	36
	10.5.2 Monitoring and reviewing factors influencing risks.....	37
10.6	Management review.....	38
10.7	Corrective action.....	38
10.8	Continual improvement.....	39
Annex A (informative) Examples of techniques in support of the risk assessment process.....		41
Bibliography.....		62

iTeh Standards
 (https://standards.iteh.ai)
 Document Preview

[SIST EN ISO/IEC 27005:2024](https://standards.iteh.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024)

<https://standards.iteh.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024>

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.

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 editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see <https://patents.iec.ch>).

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 27005:2018), which has been technically revised.

The main changes are as follows:

- all guidance text has been aligned with ISO/IEC 27001:2022, and ISO 31000:2018;
- the terminology has been aligned with the terminology in ISO 31000:2018;
- the structure of the clauses has been adjusted to the layout of ISO/IEC 27001:2022;
- risk scenario concepts have been introduced;
- the event-based approach is contrasted with the asset-based approach to risk identification;
- the content of the annexes has been revised and restructured into a single annex.

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 and www.iec.ch/national-committees.

ISO/IEC 27005:2022(E)

Introduction

This document provides guidance on:

- implementation of the information security risk requirements specified in ISO/IEC 27001;
- essential references within the standards developed by ISO/IEC JTC 1/SC 27 to support information security risk management activities;
- actions that address risks related to information security (see ISO/IEC 27001:2022, 6.1 and Clause 8);
- implementation of risk management guidance in ISO 31000 in the context of information security.

This document contains detailed guidance on risk management and supplements the guidance in ISO/IEC 27003.

This document is intended to be used by:

- organizations that intend to establish and implement an information security management system (ISMS) in accordance with ISO/IEC 27001;
- persons that perform or are involved in information security risk management (e.g. ISMS professionals, risk owners and other interested parties);
- organizations that intend to improve their information security risk management process.

ITeH Standards
(<https://standards.iteh.ai>)
Document Preview

[SIST EN ISO/IEC 27005:2024](https://standards.iteh.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024)

<https://standards.iteh.ai/catalog/standards/sist/509c590f-51c7-4f8b-a6a4-57236a8d8d91/sist-en-iso-iec-27005-2024>

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

1 Scope

This document provides guidance to assist organizations to:

- fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks;
- perform information security risk management activities, specifically information security risk assessment and treatment.

This document is applicable to all organizations, regardless of type, size or sector.

2 Normative references

The following documents are 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*

3 Terms and definitions

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

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

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

3.1 Terms related to information security risk

3.1.1

external context

external environment in which the organization seeks to achieve its objectives

Note 1 to entry: External context can include the following:

- the social, cultural, political, legal, regulatory, financial, technological, economic, geological environment, whether international, national, regional or local;
- key drivers and trends affecting the objectives of the organization;
- external interested parties' relationships, perceptions, values, needs and expectations;
- contractual relationships and commitments;
- the complexity of networks and dependencies.

[SOURCE: ISO Guide 73:2009, 3.3.1.1, modified — Note 1 to entry has been modified.]

ISO/IEC 27005:2022(E)

3.1.2

internal context

internal environment in which the organization seeks to achieve its objectives

Note 1 to entry: Internal context can include:

- vision, mission and values;
- governance, organizational structure, roles and accountabilities;
- strategy, objectives and policies;
- the organization's culture;
- standards, guidelines and models adopted by the organization;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- data, information systems and information flows;
- relationships with internal interested parties, taking into account their perceptions and values;
- contractual relationships and commitments;
- internal interdependencies and interconnections.

[SOURCE: ISO Guide 73:2009, 3.3.1.2, modified — Note 1 to entry has been modified.]

3.1.3

risk

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected, positive or negative.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an *event* (3.1.11), its *consequence* (3.1.14), or *likelihood* (3.1.13).

Note 4 to entry: Risk is usually expressed in terms of *risk sources* (3.1.6), potential events, their consequences and their likelihood.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

Note 6 to entry: Information security risks are usually associated with a negative effect of uncertainty on information security objectives.

Note 7 to entry: Information security risks can be associated with the potential that *threats* (3.1.9) will exploit *vulnerabilities* (3.1.10) of an information asset or group of information assets and thereby cause harm to an organization.

[SOURCE: ISO 31000:2018, 3.1, modified — the phrase: “It can be positive, negative or both, and can address, create or result in opportunities and threats” has been replaced with “positive or negative” in Note 1 to entry; the original Note 3 to entry has been renumbered as Note 4 to entry; and Notes 3, 5, 6 and 7 to entry have been added.]

3.1.4

risk scenario

sequence or combination of *events* (3.1.11) leading from the initial cause to the unwanted *consequence* (3.1.14)

[SOURCE: ISO 17666:2016, 3.1.13, modified — Note 1 to entry has been deleted.]