

INFOTURVE, KÜBERTURVE JA PRIVAATSUSKAITSE
Infoturvariskide haldamise juhend

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

EESTI STANDARDI EESSÕNA**NATIONAL FOREWORD**

<p>See Eesti standard EVS-ISO/IEC 27005:2024 sisaldab rahvusvahelise standardi ISO/IEC 27005:2022 „Information security, cybersecurity and privacy protection. Guidance on managing information security risks“ identset ingliskeelset teksti.</p> <p>Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus.</p> <p>Standard EVS-ISO/IEC 27005:2024 on jõustunud sellekohase teate avaldamisega EVS Teatajas.</p> <p>Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.</p>	<p>This Estonian Standard EVS-ISO/IEC 27005:2024 consists of the identical English text of the International Standard ISO/IEC 27005:2022 „Information security, cybersecurity and privacy protection. Guidance on managing information security risks“.</p> <p>Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 4, the Estonian Standard has been published by the Estonian Centre for Standardisation and Accreditation.</p> <p>Standard EVS-ISO/IEC 27005:2024 has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.</p> <p>This standard is available from the Estonian Centre for Standardisation and Accreditation.</p>
--	--

Käsitusala

See dokument annab juhiseid organisatsioonide abistamiseks

- infoturvariskide käsitlemise toiminguid puudutavate standardi ISO/IEC 27001 nõuete täitmisel;
- infoturvariski halduse tegevuste, eriti infoturvariski kontrolli ja käsitluse sooritamisel.

See dokument on kohaldatav kõigis organisatsioonides sõltumata nende tüübist, suuruselt või majandussektorist.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autoriõiguse kaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about standards copyright protection, please contact the Estonian Centre for Standardisation and Accreditation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

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	8
5.1 Information security risk management process.....	8
5.2 Information security risk management cycles.....	9
6 Context establishment	10
6.1 Organizational considerations	10
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	16
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.....	19
7.3 Analysing information security risks	19
7.3.1 General	19
7.3.2 Assessing potential consequences.....	20
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	24
8.1 General.....	24
8.2 Selecting appropriate information security risk treatment options.....	24
8.3 Determining all controls that are necessary to implement the information security risk treatment options.....	25
8.4 Comparing the controls determined with those in ISO/IEC 27001:2022, Annex A	27
8.5 Producing a Statement of Applicability	28
8.6 Information security risk treatment plan.....	29
8.6.1 Formulation of the risk treatment plan.....	29
8.6.2 Approval by risk owners.....	30
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	32

10	Leveraging related ISMS processes	32
10.1	Context of the organization	32
10.2	Leadership and commitment.....	33
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	36
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.....	64

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.

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.

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.]