SLOVENSKI STANDARD
SIST EN ISO/IEC 27007:2022

01-april-2022

Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Smernice za presojanje sistemov upravljanja informacijske varnosti (ISO/IEC 27007:2020)

Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing (ISO/IEC 27007:2020)

Informationstechnik - Sicherheitsverfahren - Leitfäden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007:2020)

Sécurité de l'information, cybersécurité et protection des données privées - Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information (ISO/IEC 27007:2020)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-8977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

Ta slovenski standard je istoveten z: **EN ISO/IEC 27007:2022**

ICS:

03.100.70	Sistemi vodenja	Management systems
03.120.20	Certificiranje proizvodov in podjetij. Ugotavljanje skladnosti	Product and company certification. Conformity assessment
35.030	Informacijska varnost	IT Security

SIST EN ISO/IEC 27007:2022 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN ISO/IEC 27007:2022

iTeh STANDARD
PREVIEW
(standards.iteh.ai)

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

SIST EN ISO/IEC 27007:2022

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 27007

January 2022

ICS 03.120.20; 35.030

English version

Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing (ISO/IEC 27007:2020)

Sécurité de l'information, cybersécurité et protection des données privées - Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information (ISO/IEC 27007:2020)

Informationstechnik - Sicherheitsverfahren - Leitfäden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007:2020)

This European Standard was approved by CEN on 26 December 2021.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 26 January 2022.

iTeh STANDARD
PREVIEW
(standards.iteh.ai)

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.

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

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, Turkey and United Kingdom.

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

© 2022 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

SIST EN ISO/IEC 27007:2022

Contents

Page

European foreword **3**

iTeh STANDARD
PREVIEW
(standards.iteh.ai)

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

SIST EN ISO/IEC 27007:2022

European foreword

The text of ISO/IEC 27007:2020 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 27007:2022 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 July 2022, and conflicting national standards shall be withdrawn at the latest by July 2022.

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, Turkey and the United Kingdom.

iTeh STANDARD
PREVIEW
(standards.iteh.ai)

Endorsement notice

The text of ISO/IEC 27007:2020 has been approved by CEN-CENELEC as EN ISO/IEC 27007:2022 without any modification.

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

SIST EN ISO/IEC 27007:2022

iTeh STANDARD
PREVIEW
(standards.iteh.ai)

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

SIST EN ISO/IEC 27007:2022

INTERNATIONAL STANDARD

ISO/IEC 27007

Third edition
2020-01

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

iTeh STANDARD
PREVIEW
(standards.iteh.ai)
SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

Reference number
ISO/IEC 27007:2020(E)

© ISO/IEC 2020

SIST EN ISO/IEC 27007:2022

iTeh STANDARD
PREVIEW
(standards.iteh.ai)

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

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

© ISO/IEC 2020 – All rights reserved

SIST EN ISO/IEC 27007:2022

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Principles of auditing **1**
5 Managing an audit programme **1**
5.1 General 1
5.2 Establishing audit programme objectives 1
5.3 Determining and evaluating audit programme risks and opportunities 2
5.4 Establishing audit programme 2
5.4.1 Roles and responsibilities of the individual(s) managing audit programme 2
5.4.2 Competence of individual(s) managing audit programme 2
5.4.3 Establishing extent of the audit programme 2
5.4.4 Determining audit programme resources 3
5.5 Implementing audit programme 3
5.5.1 General 3
5.5.2 Defining the objectives, scope and criteria for an individual audit 3
5.5.3 Selecting and determining audit methods 4
5.5.4 Selecting audit team members 4
5.5.5 Assigning responsibility for an individual audit to the audit team leader 4
5.5.6 Managing audit programme results 4
5.5.7 Managing and maintaining audit programme records 4
5.6 Monitoring audit programme 5
5.7 Reviewing and improving audit programme 5
6 Conducting an audit **5**
6.1 General 5
6.2 Initiating audit 5
6.2.1 General 5
6.2.2 Establishing contact with auditee 5
6.2.3 Determining feasibility of audit 5
6.3 Preparing audit activities 5
6.3.1 Performing review of documented information 5
6.3.2 Audit planning 5
6.3.3 Assigning work to audit team 6
6.3.4 Preparing documented information for audit 6
6.4 Conducting audit activities 6
6.4.1 General 6
6.4.2 Assigning roles and responsibilities of guides and observers 6
6.4.3 Conducting opening meeting 6
6.4.4 Communicating during audit 6
6.4.5 Audit information availability and access 6
6.4.6 Reviewing document information while conducting audit 6
6.4.7 Collecting and verifying information 7
6.4.8 Generating audit findings 7
6.4.9 Determining audit conclusions 7
6.4.10 Conducting closing meeting 7
6.5 Preparing and distributing audit report 7
6.5.1 Preparing audit report 7
6.5.2 Distributing audit report 7
6.6 Completing audit 7
6.7 Conducting audit follow-up 7

iTeh STANDARD PREVIEW (standards.iteh.ai)
SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

© ISO/IEC 2020 – All rights reserved

SIST EN ISO/IEC 27007:2022

7 Competence and evaluation of auditors **8**
7.1 General 8
7.2 Determining auditor competence 8
7.2.1 General 8
7.2.2 Personal behaviour 8
7.2.3 Knowledge and skills 8
7.2.4 Achieving auditor competence 9
7.2.5 Achieving audit team leader competence 9
7.3 Establishing auditor evaluation criteria 9
7.4 Selecting appropriate auditor evaluation method 9
7.5 Conducting auditor evaluation 9
7.6 Maintaining and improving auditor competence 9
Annex A (informative) **Guidance for ISMS auditing practice** **10**
Bibliography **39**

iTeh STANDARD
PREVIEW
(standards.iteh.ai)
SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

 © ISO/IEC 2020 – All rights reserved

SIST EN ISO/IEC 27007:2022

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).

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 http://patents.iec.ch).

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

iTeh STANDARD
PREVIEW
(standards.iteh.ai)

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.

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

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

This third edition cancels and replaces the second edition (ISO/IEC 27007:2017), which has been technically revised.

The main changes compared to the previous edition are as follows:

— the document has been aligned with ISO 19011:2018;

— the Introduction has been reworded and expanded;

— in 5.1, the entire text has been removed;

— in 5.2.2, the former item d) has been removed;

— in 5.3, the entire text has been removed;

— in 5.5.2.2, the former item b) and a paragraph below has been removed;

— in 6.5.2.2, the first paragraph has been removed and the NOTE reworded.

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.

© ISO/IEC 2020 – All rights reserved

SIST EN ISO/IEC 27007:2022

Introduction

An information security management system (ISMS) audit can be conducted against a range of audit criteria, separately or in combination, including but not limited to:

— requirements defined in ISO/IEC 27001:2013;

— policies and requirements specified by relevant interested parties;

— statutory and regulatory requirements;

— ISMS processes and controls defined by the organization or other parties;

— management system plan(s) relating to the provision of specific outputs of an ISMS (e.g. plans to address risks and opportunities when establishing ISMS, plans to achieve information security objectives, risk treatment plans, project plans).

This document provides guidance for all sizes and types of organizations and ISMS audits of varying scopes and scales, including those conducted by large audit teams, typically of larger organizations, and those by single auditors, whether in large or small organizations. This guidance should be adapted as appropriate to the scope, complexity and scale of the ISMS audit programme.

This document concentrates on ISMS internal audits (first party) and ISMS audits conducted by organizations on their external providers and other external interested parties (second party). This document can also be useful for ISMS external audits conducted for purposes other than third party management system certification. ISO/IEC 27006 provides requirements for auditing ISMS for third party certification; this document can provide useful additional guidance.

iTeh STANDARD
PREVIEW
(standards.iteh.ai)

This document is to be used in conjunction with the guidance contained in ISO 19011:2018.

This document follows the structure of ISO 19011:2018.

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

ISO 19011:2018 provides guidance on the management of audit programmes, the conduct of internal or external audits of management systems, as well as on the competence and evaluation of management system auditors.

Annex A provides guidance for ISMS auditing practices along with requirements of ISO/IEC 27001:2013, Clauses 4 to 10.

 © ISO/IEC 2020 – All rights reserved

SIST EN ISO/IEC 27007:2022

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

1 Scope

This document provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011.

This document is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

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 19011:2018, *Guidelines for auditing management systems*

ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

iTeh STANDARD PREVIEW (standards.iteh.ai)

3 Terms and definitions

SIST EN ISO/IEC 27007:2022 https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-4778-8b9d-01a1004fd574/sist-en-iso-iec-27007-2022

For the purposes of this document, the terms and definitions given in ISO 19011 and ISO/IEC 27000 apply.

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 Principles of auditing

The principles of auditing of ISO 19011:2018, Clause 4, apply.

5 Managing an audit programme

5.1 General

The guidelines of ISO 19011:2018, 5.1, apply.

5.2 Establishing audit programme objectives

5.2.1 The guidelines of ISO 19011:2018, 5.2, apply. In addition, the guidance in 5.2.2 applies.

© ISO/IEC 2020 – All rights reserved

SIST EN ISO/IEC 27007:2022

5.2.2 ISMS-specific considerations for determining audit[1)] programme objectives can include:

a) identified information security requirements;

b) requirements of ISO/IEC 27001;

c) auditee's level of performance, as reflected in the occurrence of information security events and incidents and effectiveness of the ISMS;

NOTE Further information about performance monitoring, measurement, analysis and evaluation can be found in ISO/IEC 27004.

d) information security risks to the relevant parties, i.e. the auditee and audit client.

Examples of ISMS-specific audit programme objectives include:

— demonstrate conformity with all relevant legal and contractual requirements and other requirements and their security implications;

— obtain and maintain confidence in the risk management capability of the auditee;

— evaluate the effectiveness of the actions to address information security risks and opportunities.

5.3 Determining and evaluating audit programme risks and opportunities

iTeh STANDARD
PREVIEW

5.3.1 The guidelines of ISO 19011:2018, 5.3, apply.

5.3.2 Measures to ensure information security and confidentiality should be determined considering auditees and other relevant party requirements. Other party requirements can include relevant legal and contractual requirements.

(standards.iteh.ai)

5.4 Establishing audit programme

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3c5bc129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

5.4.1 Roles and responsibilities of the individual(s) managing audit programme

The guidelines of ISO 19011:2018, 5.4.1, apply. In addition, the guidance in 5.4.1.2 applies.

5.4.2 Competence of individual(s) managing audit programme

The guidelines of ISO 19011:2018, 5.4.2, apply.

5.4.3 Establishing extent of the audit programme

5.4.3.1 The guidelines of ISO 19011:2018, 5.4.3, apply. In addition, the guidance in 5.4.3.2 applies.

5.4.3.2 The extent of an audit programme can include the following:

a) the size of the ISMS, including:

1) the total number of persons doing work under the organization's control and relationships with interested parties and contractors that are relevant to the ISMS;

2) the number of information systems;

1) For the purpose of this document, the term "audit" refers to ISMS audits.

© ISO/IEC 2020 – All rights reserved

SIST EN ISO/IEC 27007:2022

3) the number of sites covered by the ISMS;

b) the complexity of the ISMS (including the number and criticality of processes and activities) taking into account differences between sites within the ISMS scope;

c) the significance of the information security risks identified for the ISMS in relation to the business;

d) the significance of the risks and opportunities determined when planning the ISMS;

e) the importance of preserving the confidentiality, integrity and availability of information within the scope of the ISMS;

f) the complexity of the information systems to be audited, including complexity of information technology deployed;

g) the number of similar sites.

Consideration should be given in the audit programme to setting priorities that warrant more detailed examination based on the significance of information security risks and business requirements in respect to the scope of the ISMS.

NOTE Further information about determining audit time can be found in ISO/IEC 27006. Further information on multi-site sampling can be found in ISO/IEC 27006 and mandatory document 1 from the International Accreditation Forum (IAF MD1, see Reference [11]). The information contained in ISO/IEC 27006 and IAF MD 1 only relates to certification audits.

iTeh STANDARD PREVIEW (standards.iteh.ai)

5.4.4 Determining audit programme resources

5.4.4.1 The guidelines of ISO 19011:2018, 5.4.4, apply. In addition, the guidance in 5.4.4.2 applies.

5.4.4.2 In particular, for all significant risks applicable to the auditee and relevant to the audit programme objectives, ISMS auditors should be allocated sufficient time to review the effectiveness of the actions to address information security risks and ISMS related risks and opportunities.

SIST EN ISO/IEC 27007:2022
https://standards.iteh.ai/catalog/standards/sist/3e58e129-b977-477b-8b9d-01a10047d574/sist-en-iso-iec-27007-2022

5.5 Implementing audit programme

5.5.1 General

The guidelines of ISO 19011:2018, 5.5.1, apply.

5.5.2 Defining the objectives, scope and criteria for an individual audit

5.5.2.1 The guidelines of ISO 19011:2018, 5.5.2, apply. In addition, the guidance in 5.5.2.2 applies.

5.5.2.2 The audit objectives may include the following:

a) evaluation of whether the ISMS adequately identifies and addresses information security requirements;

b) determination of the extent of conformity of information security controls with the requirements and procedures of the ISMS.

The audit scope should take into account information security risks and relevant risks and opportunities affecting the ISMS of relevant parties, i.e. the audit client and the auditee.

© ISO/IEC 2020 – All rights reserved