SLOVENSKI STANDARD
SIST ISO/IEC 27007:2018

01-september-2018

Nadomešča:

SIST ISO/IEC 27007:2015

Informacijska tehnologija - Varnostne tehnike - Smernice za presojanje sistemov upravljanja informacijske varnosti

Information technology - Security techniques - Guidelines for information security management systems auditing

Technologies de l'information - Techniques de sécurité - Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Ta slovenski standard je istoveten z: **ISO/IEC 27007:2017**

ICS:

03.100.70	Sistemi vodenja	Management systems
35.030	Informacijska varnost	IT Security

SIST ISO/IEC 27007:2018 **en,fr,de**

INTERNATIONAL STANDARD

ISO/IEC 27007

Second edition
2017-10

Information technology — Security techniques — Guidelines for information security management systems auditing

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27007:2017(E)

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

Contents

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.

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 ISO documents 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 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.

This document 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 27007:2011), which has been technically revised.

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

— Annex A has been completely reworked to align to ISO/IEC 27001:2013;

— the main part of this document has been aligned with ISO/IEC 27001:2013.

Introduction

This document provides guidance on:

a) the management of an information security management system (ISMS) audit programme;

b) the conduct of internal and external ISMS audits in accordance with ISO/IEC 27001;

c) the competence and evaluation of ISMS auditors.

This document should be used in conjunction with the guidance contained in ISO 19011:2011.

This document follows the structure of ISO 19011:2011. Additional ISMS-specific guidance on the application of ISO 19011:2011 for ISMS audits is identified by the letters “IS”.

ISO 19011:2011 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.

NOTE For accredited certification, auditor requirements are given in ISO/IEC 27006.

This document does not state requirements and is intended for all users, including small and medium-sized organizations.

Information technology — Security techniques — 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 19011:2011.

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 19011:2011, *Guidelines for auditing management systems*

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *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 19011:2011 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 http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Principles of auditing

The principles of auditing of ISO 19011:2011, Clause 4 apply.

5 Managing an audit programme

5.1 General

The guidelines of ISO 19011:2011, 5.1 apply. In addition, the following guidance applies.

5.1.1 IS 5.1 General

An organization needing to conduct audits should establish the audit[1] programme, taking account of the risks and opportunities determined when planning the ISMS.

5.2 Establishing the audit programme objectives

The guidelines of ISO 19011:2011, 5.2 apply. In addition, the following guidance applies.

5.2.1 IS 5.2 Establishing the audit programme objectives

ISMS-specific considerations for determining audit 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) risks and opportunities determined when planning the ISMS of the auditee;

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

Examples of ISMS-specific audit programme objectives include:

— verification of conformity with the relevant legal and contractual requirements and other requirements and their security implications;

— obtaining and maintaining confidence in the risk management capability of the auditee;

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

5.3 Establishing the audit programme

5.3.1 Role and responsibilities of the person managing the audit programme

The guidelines of ISO 19011:2011, 5.3.1 apply.

5.3.2 Competence of the person managing the audit programme

The guidelines of ISO 19011:2011, 5.3.2 apply.

5.3.3 Establishing the extent of the audit programme

The guidelines of ISO 19011:2011, 5.3.3 apply. In addition, the following guidance applies.

5.3.3.1 IS 5.3.3 Establishing the extent of the audit programme

The extent of an audit programme can vary and can be influenced by the following factors:

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;

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

2) the number of information systems;

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 [12]). The information contained in ISO/IEC 27006 and IAF MD 1 only relates to certification audits.

5.3.4 Identifying and evaluating audit programme risks

The guidelines of ISO 19011:2011, 5.3.4 apply. In addition, the following guidance applies.

5.3.4.1 IS 5.3.4 Identifying and evaluating audit programme risks

Audit programme risks can be additionally associated with risks related to confidentiality requirements.

5.3.5 Establishing procedures for the audit programme

The guidelines of ISO 19011:2011, 5.3.5 apply. In addition, the following guidance applies.

5.3.5.1 IS 5.3.5 Establishing procedures for the audit programme

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.

5.3.6 Identifying audit programme resources

The guidelines of ISO 19011:2011, 5.3.6 apply. In addition, the following guidance applies.

5.3.6.1 IS 5.3.6 Identifying audit programme resources

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.

5.4 Implementing the audit programme

5.4.1 General

The guidelines of ISO 19011:2011, 5.4.1 apply

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

The guidelines of ISO 19011:2011, 5.4.2 apply. In addition, the following guidance applies.

5.4.2.1 IS 5.4.2 Defining the objectives, scope and criteria for an individual audit

The audit objectives can include the following:

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

b) evaluation of the processes for the maintenance and effective improvement of the ISMS;

c) 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.

If ISMS is in the scope of the audit, then the audit team should verify that the scope and boundaries of the ISMS of the auditee are clearly defined based on internal and external issues and the needs and expectations of interested parties. The audit team should confirm that the auditee addresses the requirements stated in ISO/IEC 27001:2013, 4.3 within the scope of the ISMS, as relevant to the audit scope.

The following topics can be considered as audit criteria and used as a reference against which conformity is determined:

a) the information security policy, information security objectives, policies and procedures adopted by the auditee;

b) legal and contractual requirements and other requirements relevant to the auditee;

c) the auditee's information security risk criteria, information security risk assessment process and risk treatment process;

d) the Statement of Applicability, the identification of any sector-specific or other necessary controls, justification for inclusions, whether they are implemented or not and the justification for exclusions of controls of ISO/IEC 27001:2013, Annex A;

e) the definition of controls to treat risks appropriately;

f) the methods and criteria for monitoring, measurement, analysis and evaluation of the information security performance and the effectiveness of the ISMS;

g) information security requirements provided by a customer;

h) information security requirements applied by a supplier or outsourcer.

5.4.3 Selecting the audit methods

The guidelines of ISO 19011:2011, 5.4.3 apply. In addition, the following guidance applies.

5.4.3.1 IS 5.4.3 Selecting the audit methods

If a joint audit is conducted, particular attention should be paid to the disclosure of information between the relevant parties. Agreement on this should be reached with all interested parties before the audit commences.

5.4.4 Selecting the audit team members

The guidelines of ISO 19011:2011, 5.4.4 apply. In addition, the following guidance applies.

5.4.4.1 IS 5.4.4 Selecting the audit team members

The competence of the overall audit team should include adequate knowledge and understanding of:

a) information security risk management sufficient to evaluate the methods used by the auditee;

b) information security and information security management sufficient to evaluate control determination, planning, implementation, maintenance and effectiveness of the ISMS.

5.4.5 Assigning responsibility for an individual audit to the audit team leader

The guidelines of ISO 19011:2011, 5.4.5 apply.

5.4.6 Managing the audit programme outcome

The guidelines of ISO 19011:2011, 5.4.6 apply.

5.4.7 Managing and maintaining audit programme records

The guidelines of ISO 19011:2011, 5.4.7 apply.

5.5 Monitoring the audit programme

The guidelines of ISO 19011:2011, 5.5 apply.

5.6 Reviewing and improving the audit programme

The guidelines of ISO 19011:2011, 5.6 apply.

6 Performing an audit

6.1 General

The guidelines of ISO 19011:2011, 6.1 apply.

6.2 Initiating the audit

6.2.1 General

The guidelines of ISO 19011:2011, 6.2.1 apply.

6.2.2 Establishing initial contact with the auditee

The guidelines of ISO 19011:2011, 6.2.2 apply. In addition, the following guidance applies.