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

Reference number
ISO/IEC 27007:2020(E)

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

Contents

Page

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.

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*.

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.

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.

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.

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.

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*

3 Terms and definitions

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.

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

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.

5.4 Establishing audit programme

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.

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.

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.

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.

The following topics may 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) 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.

5.5.3 Selecting and determining audit methods

5.5.3.1 The guidelines of ISO 19011:2018, 5.5.3, apply. In addition, the guidance in 5.5.3.2 applies.

5.5.3.2 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.

5.5.4 Selecting audit team members

5.5.4.1 The guidelines of ISO 19011:2018, 5.5.4, apply. In addition, the guidance in 5.5.4.2 applies.

5.5.4.2 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.

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

The guidelines of ISO 19011:2018, 5.5.5, apply.

5.5.6 Managing audit programme results

The guidelines of ISO 19011:2018, 5.5.6, apply.

5.5.7 Managing and maintaining audit programme records

The guidelines of ISO 19011:2018, 5.5.7, apply.

5.6 Monitoring audit programme

The guidelines of ISO 19011:2018, 5.6, apply.

5.7 Reviewing and improving audit programme

The guidelines of ISO 19011:2018, 5.7, apply.

6 Conducting an audit

6.1 General

The guidelines of ISO 19011:2018, 6.1, apply.

6.2 Initiating audit

6.2.1 General

The guidelines of ISO 19011:2018, 6.2.1, apply.

6.2.2 Establishing contact with auditee

6.2.2.1 The guidelines of ISO 19011:2018, 6.2.2, apply. In addition, the guidance in 6.2.2.2 applies.

6.2.2.2 Where necessary, care should be taken to ensure that the auditors have obtained the necessary security clearance to access documented information or other information required for audit activities (including but not limited to confidential or sensitive information).

6.2.3 Determining feasibility of audit

6.2.3.1 The guidelines of ISO 19011:2018, 6.2.3, apply. In addition, the guidance in 6.2.3.2 applies.

6.2.3.2 Before the audit commences, the auditee should be asked whether any ISMS audit evidence is unavailable for review by the audit team, e.g. because the evidence contains personally identifiable information or other confidential/sensitive information. The person responsible for managing the audit programme should determine whether the ISMS can be adequately audited in the absence of audit evidence. If the conclusion is that it is not possible to adequately audit the ISMS without reviewing the identified audit evidence, the person responsible for managing the audit programme should advise the auditee that the audit cannot take place until appropriate access arrangements are granted or alternative means to achieve the audit have been proposed to or by the auditee. If the audit proceeds, the audit plan should take into account any access limitations.

6.3 Preparing audit activities

6.3.1 Performing review of documented information

The guidelines of ISO 19011:2018, 6.3.1, apply.

6.3.2 Audit planning

6.3.2.1 The guidelines of ISO 19011:2018, 6.3.2, apply. In addition, the guidance in 6.3.2.2 applies.

6.3.2.2 The audit team leader should be aware that risks to the auditee can result from the presence of the audit team members. The audit team's presence can influence information security and present

a source of additional risk to the auditee's information, e.g. confidential or sensitive records or system infrastructure (e.g. accidental erasure, unauthorized disclosure of information, unintended alteration of information).

6.3.3 Assigning work to audit team

The guidelines of ISO 19011:2018, 6.3.3, apply.

6.3.4 Preparing documented information for audit

6.3.4.1 The guidelines of ISO 19011:2018, 6.3.4, apply. In addition, the guidance in 6.3.4.2 applies.

6.3.4.2 The audit team leader should ensure all audit work documents are classified appropriately and handled in accordance with that classification.

6.4 Conducting audit activities

6.4.1 General

The guidelines of ISO 19011:2018, 6.4.1, apply.

6.4.2 Assigning roles and responsibilities of guides and observers

The guidelines of ISO 19011:2018, 6.4.2, apply.

6.4.3 Conducting opening meeting

The guidelines of ISO 19011:2018, 6.4.3, apply.

6.4.4 Communicating during audit

The guidelines of ISO 19011:2018, 6.4.4, apply.

6.4.5 Audit information availability and access

6.4.5.1 The guidelines of ISO 19011:2018, 6.4.5, apply. In addition, the guidance in 6.4.5.2 applies.

6.4.5.2 If any audit evidence is not available to the audit team during the audit for reasons of classification or sensitivity, the lead auditor should determine the extent to which this affects the confidence in the audit findings and conclusion, and reflect on it in the audit report without compromising the sensitivity of the evidence that was not available.

6.4.6 Reviewing document information while conducting audit

6.4.6.1 The guidelines of ISO 19011:2018, 6.4.6, apply. In addition, the guidance in 6.4.6.2 applies.

6.4.6.2 ISMS Auditors should verify that documented information as required by the audit criteria and relevant to the audit scope exists and conforms to the audit criteria requirements.

ISMS Auditors should confirm that the determined controls within the scope of the audit are related to the results of the risk assessment and risk treatment process, and can subsequently be traced back to the information security policy and objectives.

NOTE Annex A provides guidance for ISMS auditing practice, including how to audit the ISMS using relevant documented information.