INTERNATIONAL STANDARD

ISO/IEC 27007

First edition
2011-11-15

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 27007:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27007 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This International Standard provides guidance on the management of an information security management system (ISMS) audit programme and the conduct of the internal or external audits in accordance with ISO/IEC 27001:2005, as well as guidance on the competence and evaluation of ISMS auditors, which should be used in conjunction with the guidance contained in ISO 19011. This International Standard does not state requirements.

This guidance is intended for all users, including small and medium sized organizations.

ISO 19011, *Guidelines for auditing management systems* 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.

The text in this International Standard follows the structure of ISO 19011, and the additional ISMS-specific guidance on the application of ISO 19011 for ISMS audits is identified by the letters “IS”.

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

1 Scope

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

This International Standard 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 referenced documents are indispensable for the application 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 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27000:2009, *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.

4 Principles of auditing

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

5 Managing an audit programme

5.1 General

The guidelines from ISO 19011:2011, Clause 5.1, apply. In addition, the following ISMS-specific guidance applies.

5.1.1 IS 5.1 General

The ISMS audit[1] programme should be developed based on the auditee's information security risk situation.

5.2 Establishing the audit programme objectives

The guidelines from ISO 19011:2011, Clause 5.2, apply. In addition, the following ISMS-specific guidance applies.

5.2.1 IS 5.2 Establishing the audit programme objectives

Objectives for audit programme(s) should be established to direct the planning and conduct of audits and to ensure that the audit programme is implemented effectively. These objectives can be dependent on:

a) identified information security requirements;
b) requirements from ISO/IEC 27001;
c) auditee's level of performance, as reflected in the occurrence of information security failures, incidents and effectiveness measurements; and
d) information security risks to the organization being audited.

Examples of audit programme objectives may include the following:

1) verification of conformity with the identified legal and contractual requirements and other requirements and their security implications;
2) Obtaining and maintaining confidence in the risk management capability of an auditee.

5.3 Establishing the audit programme

5.3.1 Role and responsibilities of the person managing the audit programme

The guidelines from ISO 19011:2011, Clause 5.3.1, apply.

5.3.2 Competence of the person managing the audit programme

The guidelines from ISO 19011:2011, Clause 5.3.2, apply.

5.3.3 Determining the extent of the audit programme

The guidelines from ISO 19011:2011, Clause 5.3.3, apply. In addition, the following ISMS-specific guidance applies.

5.3.3.1 IS 5.3.3 Determining the extent of the audit programme

The extent of an audit programme can vary. Factors that can influence the extent of the audit programme are:

a) the size of the ISMS, including
    1. the total number of personnel working at each location and relationships with third-party contractors working regularly at the location to be audited;
    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);
c) the significance of the information security risks identified for the ISMS;
d) the importance of information and related assets within the scope of the ISMS;

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

e) the complexity of the information systems to be audited on site, including complexity of information technology deployed;
f) whether there are many similar sites; and
g) the variations in ISMS complexity across the sites in scope.

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

Further information about multi-site sampling can be found in ISO/IEC 27006:2007 and IAF MD 1:2007 (see Bibliography), where the information in these documents only relates to certification audits.

5.3.4 Identifying and evaluating audit programme risks

The guidelines from ISO 19011:2011, Clause 5.3.4, apply.

5.3.5 Establishing procedures for the audit programme

The guidelines from ISO 19011:2011, Clause 5.3.5, apply.

5.3.6 Identifying audit programme resources

The guidelines from ISO 19011:2011, Clause 5.3.6, apply. In addition, the following ISMS-specific guidance applies.

5.3.6.1 IS 5.3.6 Identifying audit programme resources

In particular, for all significant risks applicable to the auditee, auditors should be allocated sufficient time to verify the effectiveness of the corresponding risk mitigation action.

5.4 Implementing the audit programme

5.4.1 General

The guidelines from ISO 19011:2011, Clause 5.4.1, apply. In addition, the following ISMS-specific guidance applies.

5.4.1.1 IS 5.4.1 General

Where applicable, confidentiality requirements of auditees and other relevant parties, including possible legal and contractual requirements, should be addressed in the implementation of an audit programme.

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

The guidelines from ISO 19011:2011, Clause 5.4.2, apply. In addition, the following ISMS-specific guidance applies.

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

The audit scope should reflect the auditee's information security risks, relevant business requirements and business risks.

The audit objectives may in addition include the following:

a) evaluation of whether the ISMS adequately identifies and addresses information security requirements;
b) evaluation of the continual suitability of the ISMS objectives defined by management; and
c) evaluation of the processes for the maintenance and effective improvement of the ISMS.

Practical help — Examples of audit criteria

The following are topics for consideration as audit criteria:

1) the auditee's information security risk assessment methodology and risk assessment and treatment results, and that these address all relevant requirements;
2) the version of the Statement of Applicability, and its relation to the results of the risk assessment;
3) the effective implementation of controls to reduce risks:
4) measurement of the effectiveness of the implemented controls, and that these measurements have been applied as defined to measure control effectiveness (see ISO/IEC 27004);
5) activities to monitor and review the ISMS processes and controls;
6) internal ISMS audits and management reviews and the organization's corrective actions;
7) information about the adequacy of and compliance with the objectives, policies, and procedures adopted by the auditee; and
8) compliance with specific legal and contractual requirements and other requirements relevant to the auditee, and their information security implications.

The audit team should ensure that the scope and boundaries of the ISMS of the auditee are clearly defined in terms of the characteristics of the business, the organization, its location, assets and technology including details and justification of any exclusion to scope. The audit team should confirm that the auditee address the requirements stated in Clause 1.2 of ISO/IEC 27001:2005 within the scope of the ISMS.

Auditors should therefore ensure that the auditee's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of the scope. Auditors should confirm that this is reflected in the Statement of Applicability.

Auditors should also ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS and are included in the auditee's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems) with other organizations.

5.4.3 Selecting the audit methods

The guidelines from ISO 19011:2011, Clause 5.4.3, apply. In addition, the following ISMS-specific 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 during the audit. Agreement on this should be reached with all interested parties before the audit commences.

5.4.4 Selecting the audit team members

The guidelines from ISO 19011:2011, Clause 5.4.4, apply. In addition, the following ISMS-specific guidance applies.

5.4.4.1 IS 5.4.4 Selecting the audit team members

The competence of the overall audit team should include:

a) adequate knowledge and understanding of information security risk management, sufficient to evaluate the methods used by the auditee; and
b) adequate knowledge and understanding of information security and information security management sufficient to evaluate control selection, and planning, implementation, maintenance and effectiveness of the ISMS.

Where necessary, care should be taken that the auditors have obtained the necessary clearance to access audit evidence.

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

The guidelines from ISO 19011:2011, Clause 5.4.5, apply.

5.4.6 Managing the audit programme outcome

The guidelines from ISO 19011:2011, Clause 5.4.6, apply.

5.4.7 Managing and maintaining audit programme records

The guidelines from ISO 19011:2011, Clause 5.4.7, apply.

5.5 Monitoring the audit programme

The guidelines from ISO 19011:2011, Clause 5.5 apply.

5.6 Reviewing and improving the audit programme

The guidelines from ISO 19011:2011, Clause 5.6 apply.

6 Performing an audit

6.1 General

The guidelines from ISO 19011:2011, Clause 6.1 apply.

6.2 Initiating the audit

6.2.1 General

The guidelines from ISO 19011:2011, Clause 6.2.1, apply.

6.2.2 Establishing initial contact with the auditee

The guidelines from ISO 19011:2011, Clause 6.2.2, apply.

6.2.3 Determining the feasibility of the audit

The guidelines from ISO 19011:2011, Clause 6.2.3, apply. In addition, the following ISMS-specific guidance applies.

6.2.3.1 IS 6.2.3 Determining the feasibility of the audit

Before the audit commences, the auditee should be asked whether any ISMS records are unavailable for review by the audit team, e.g. because they contain confidential or sensitive information. The person responsible for managing the audit programme should determine whether the ISMS can be adequately audited in the absence of these records. If the conclusion is that it is not possible to adequately audit the ISMS without reviewing the identified records, the person should advise the auditee that the audit cannot take place until appropriate access arrangements are granted and an alternative could be proposed to or by the auditee.

6.3 Preparing audit activities

6.3.1 Performing document review in preparation for the audit

The guidelines from ISO 19011:2011, Clause 6.3.1, apply.

6.3.2 Preparing the audit plan

The guidelines from ISO 19011:2011, Clause 6.3.2, apply.

6.3.3 Assigning work to the audit team

The guidelines from ISO 19011:2011, Clause 6.3.3, apply.

6.3.4 Preparing work documents

The guidelines from ISO 19011:2011, Clause 6.3.4, apply.

6.4 Conducting the audit activities

6.4.1 General

The guidelines from ISO 19011:2011, Clause 6.4.1, apply.

6.4.2 Conducting the opening meeting

The guidelines from ISO 19011:2011, Clause 6.4.2, apply.

6.4.3 Performing document review while conducting the audit

The guidelines from ISO 19011:2011, Clause 6.4.3 apply. In addition, the following ISMS-specific guidance applies.

6.4.3.1 IS 6.4.3 Performing document review while conducting the audit

Auditors should check that documents required by ISO/IEC 27001 exist and conform to its requirements.

Auditors should confirm that the selected controls are related to the results of the risk assessment and risk treatment process, and can subsequently be traced back to the ISMS policy and objectives.

NOTE Annex A of this standard provides guidance on how to audit the ISMS processes and ISMS documentation.

6.4.4 Communicating during the audit

The guidelines from ISO 19011:2011, Clause 6.4.4, apply.

6.4.5 Assigning roles and responsibilities of guides and observers

The guidelines from ISO 19011:2011, Clause 6.4.5, apply.

6.4.6 Collecting and verifying information

The guidelines from ISO 19011:2011, Clause 6.4.6, apply. In addition, the following ISMS-specific guidance applies.