INTERNATIONAL STANDARD

ISO/IEC 27006

Second edition
2011-12-01

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27006:2011(E)

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 27006 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 27006:2007), which has been technically revised.

Introduction

ISO/IEC 17021 sets out criteria for bodies operating audit and certification of organizations' management systems. If such bodies are to be accredited as complying with ISO/IEC 17021 with the objective of auditing and certifying information security management systems (ISMS) in accordance with ISO/IEC 27001:2005, some additional requirements and guidance to ISO/IEC 17021 are necessary. These are provided by this International Standard.

The text in this International Standard follows the structure of ISO/IEC 17021, and the additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021 for ISMS certification are identified by the letters “IS”.

The term “shall” is used throughout this International Standard to indicate those provisions which, reflecting the requirements of ISO/IEC 17021 and ISO/IEC 27001, are mandatory. The term “should” is used to indicate recommendation.

One aim of this International Standard is to enable accreditation bodies to more effectively harmonize their application of the standards against which they are bound to assess certification bodies.

NOTE Throughout this International Standard, the terms “management system” and “system” are used interchangeably. The definition of a management system can be found in ISO 9000:2005. The management system as used in this International Standard is not to be confused with other types of system, such as IT systems.

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

1 Scope

This International Standard specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

The requirements contained in this International Standard need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in this International Standard provides additional interpretation of these requirements for any body providing ISMS certification.

NOTE This International Standard can be used as a criteria document for accreditation, peer assessment or other audit processes.

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/IEC 17021:2011, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO 19011, *Guidelines for auditing management systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021, ISO/IEC 27001 and the following apply.

3.1
certificate
certificate issued by a certification body in accordance with the conditions of its accreditation and bearing an accreditation symbol or statement

3.2
certification body
third party that assesses and certifies the ISMS of a client organization with respect to published ISMS standards, and any supplementary documentation required under the system

3.3
certification document
document indicating that a client organization's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system

3.4
mark
legally registered trade mark or otherwise protected symbol which is issued under the rules of an accreditation body or of a certification body, indicating that adequate confidence in the systems operated by a body has been demonstrated or that relevant products or individuals conform to the requirements of a specified standard

3.5
organization
company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration and is able to ensure that information security is exercised

4 Principles

The principles from ISO/IEC 17021:2011, Clause 4 apply.

5 General requirements

5.1 Legal and contractual matter

The requirements from ISO/IEC 17021:2011, Clause 5.1 apply.

5.2 Management of impartiality

The requirements from ISO/IEC 17021:2011, Clause 5.2 apply. In addition, the following ISMS-specific requirements and guidance apply.

5.2.1 IS 5.2 Conflicts of interest

Certification bodies can carry out the following duties without them being considered as consultancy or having a potential conflict of interest:

a) certification, including information meetings, planning meetings, examination of documents, auditing (not internal ISMS auditing or internal security reviews) and follow up of non-conformities;

b) arranging and participating as a lecturer in training courses, provided that, where these courses relate to information security management, related management systems or auditing, certification bodies shall confine themselves to the provision of generic information and advice which is freely available in the public domain, i.e. they shall not provide company-specific advice which contravenes the requirements of c) below;

c) making available or publishing on request information describing the certification body's interpretation of the requirements of the certification audit standards (see 9.1.1.1);

d) activities prior to audit, solely aimed at determining readiness for certification audit; however, such activities shall not result in the provision of recommendations or advice that would contravene this clause and the certification body shall be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual certification audit duration;

e) performing second and third party audits according to standards or regulations other than those being part of the scope of accreditation;

f) adding value during certification audits and surveillance visits, e.g., by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions.

The certification body shall be independent from the body or bodies (including any individuals) which provide the internal ISMS audit of the client organization's ISMS subject to certification.

5.3 Liability and financing

The requirements from ISO/IEC 17021:2011, Clause 5.3 apply.

6 Structural requirements

6.1 Organizational structure and top management

The requirements from ISO/IEC 17021:2011, Clause 6.1 apply.

6.2 Committee for safeguarding impartiality

The requirements from ISO/IEC 17021:2011, Clause 6.2 apply.

7 Resource requirements

7.1 Competence of management and personnel

The requirements from ISO/IEC 17021:2011, Clause 7.1 apply. In addition, the following ISMS-specific requirements and guidance apply.

7.1.1 IS 7.1.1 General considerations

The essential elements of competence required to perform ISMS certification are to select, provide and manage those individuals whose skills and collective competence is appropriate to the activities to be audited and the related information security issues.

7.1.1.1 Competence analysis and contract review

The certification body shall ensure that it has knowledge of the technological and legal developments relevant to the ISMS of the client organization, which it assesses.

The certification body shall have an effective system for the analysis of the competencies in information security management which it needs to have available, with respect to all the technical areas in which it operates.

For each client, the certification body shall be able to demonstrate that it has performed a competence analysis (assessment of skills in response to evaluated needs) of the requirements of each relevant sector prior to undertaking the contract review. The certification body shall then review the contract with the client organization, based on the results of this competence analysis. In particular, the certification body shall be able to demonstrate that it has the competence to complete the following activities:

a) understand the areas of activity of the client organization and the associated business risks;

b) define the competencies needed in the certification body to certify in relation to the identified activities, and information security related threats to assets, vulnerabilities and impacts on the client organization;

c) confirm the availability of the required competencies.

7.1.1.2 Resources

The management of the certification body shall have the necessary processes and resources to enable it to determine whether or not individual auditors are competent for the tasks they are required to perform within the scope of certification in which they are operating. The competence of auditors may be established by verified background experience and specific training or briefing (see also Annex B). The certification body shall be able to communicate effectively with all those clients it provides services to.

7.1.2 IS 7.1.2 Determination of Competence Criteria

Additional information on knowledge and skills is provided in Annex B to support the competence criteria of ISO/IEC 17021.

7.2 Personnel involved in the certification activities

The requirements from ISO/IEC 17021:2011, Clause 7.2 apply. In addition, the following ISMS-specific requirements and guidance apply.

7.2.1 IS 7.2 Competence of certification body personnel

Certification bodies shall have personnel competent to

a) select and verify the competence of ISMS auditors for audit teams appropriate for the audit;

b) brief ISMS auditors and arrange any necessary training;

c) decide on the granting, maintaining, withdrawing, suspending, extending, or reducing of certifications;

d) set up and operate an appeals and complaints process.

7.2.1.1 Training of audit teams

The certification body shall have criteria for the training of audit teams that ensures

a) knowledge of the ISMS standard and other relevant normative documents;

b) understanding of information security;

c) understanding of risk assessment and risk management from the business perspective;

d) technical knowledge of the activity to be audited;

e) general knowledge of regulatory requirements relevant to ISMSs;

f) knowledge of management systems;

g) understanding of the principles of auditing based on ISO 19011;

h) knowledge of ISMS effectiveness review and measurement of control effectiveness.

These training requirements apply to all members of the audit team, with the exception of d), which can be shared among members of the audit team.

7.2.1.1.1 When selecting the audit team to be appointed for a specific certification audit the certification body shall ensure that the skills brought to each assignment are appropriate. The team shall

a) have appropriate technical knowledge of the specific activities within the scope of the ISMS for which certification is sought and, where relevant, with associated procedures and their potential information security risks (technical experts who are not auditors may fulfil this function);

b) have a sufficient degree of understanding of the client organization to conduct a reliable certification audit of its ISMS in managing the information security aspects of its activities, products and services;

c) have appropriate understanding of the regulatory requirements applicable to the client organization's ISMS.

7.2.1.1.2 When required, the audit team may be complemented by technical experts who can demonstrate specific competence in a field of technology appropriate to the audit. Note should be taken that technical experts cannot be used in place of ISMS auditors but could advise auditors on matters of technical adequacy in the context of the management system being subjected to audit. The certification body shall have a procedure for

a) selecting auditors and technical experts on the basis of their competence, training, qualifications and experience;

b) initially assessing the conduct of auditors and technical experts during certification audits and subsequently monitoring the performance of auditors and technical experts.

7.2.1.2 Management of the decision taking process

The management function shall have the technical competence and ability in place to manage the process of decision-making regarding the granting, maintaining, extending, reducing, suspending and withdrawing of ISMS certification to the requirements of ISO/IEC 27001.

7.2.1.3 Pre-requisite levels of education, work experience, auditor training and audit experience for auditors conducting ISMS audits

7.2.1.3.1 The following criteria shall be applied for each auditor in the ISMS audit team. The auditor shall

a) have an education at secondary level;

b) have at least four years full time practical workplace experience in information technology, of which at least two years are in a role or function relating to information security;

c) have successfully completed five days of training, the scope of which covers ISMS audits and audit management shall be considered appropriate;

d) have gained experience in the entire process of assessing information security prior to assuming responsibility for performing as an auditor. This experience should have been gained by participation in a minimum of four certification audits for a total of at least 20 days, including review of documentation and risk analysis, implementation assessment and audit reporting;

e) have experience which is reasonably current;

f) be able to put complex operations in a broad perspective and to understand the role of individual units in larger client organizations;

g) keep their knowledge and skills in information security and auditing up to date through continual professional development.

Technical experts shall comply with criteria a), b), e) and f).

7.2.1.3.2 In addition to the requirements in 7.2.1.3.1, audit team leaders shall fulfil the following requirements, which shall be demonstrated in audits under guidance and supervision:

a) have knowledge and skills to manage the certification audit process;

b) have been an auditor in at least three complete ISMS audits;

c) have demonstrated the capability to communicate effectively, both orally and in writing.

7.3 Use of individual external auditors and external technical experts

The requirements from ISO/IEC 17021:2011, Clause 7.3 apply. In addition, the following ISMS-specific requirements and guidance applies.

7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team

When using individual external auditors or external technical experts as part of the audit team, the certification body shall ensure that they are competent and comply with the applicable provisions of this publication and are not involved, either directly or through its employer with the design, implementation or maintenance of an ISMS or related management system(s) in such a way that impartiality could be compromised.

7.3.1.1 Use of technical experts

Technical experts with specific knowledge regarding the process and information security issues and legislation affecting the client organization, but who do not satisfy all of the criteria in 7.2, may be part of the audit team. Technical experts shall work under the supervision of an auditor.

7.4 Personnel records

The requirements from ISO/IEC 17021:2011, Clause 7.4 apply.

7.5 Outsourcing

The requirements from ISO/IEC 17021:2011, Clause 7.5 apply.

8 Information requirements

8.1 Publicly accessible information

The requirements from ISO/IEC 17021:2011, Clause 8.1 apply. In addition, the following ISMS-specific requirements and guidance apply.

8.1.1 IS 8.1 Procedures for granting, maintaining, extending, reducing, suspending and withdrawing certification

The certification body shall require the client organization to have a documented and implemented ISMS which conforms to ISO/IEC 27001 and other documents required for certification.

The certification body shall have documented procedures for

a) the initial certification audit of a client organization's ISMS, in accordance with the provisions of ISO/IEC 17021 and other relevant documents;

b) surveillance and recertification audits of a client organization's ISMS in accordance with ISO/IEC 17021 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that a client organization takes corrective action on a timely basis to correct all nonconformities.

8.2 Certification documents

The requirements from ISO/IEC 17021:2011, Clause 8.2 apply. In addition, the following ISMS-specific requirements and guidance apply.

8.2.1 IS 8.2 ISMS Certification documents

The certification body shall provide to each of its client organizations whose ISMS is certified, certification documents such as a letter or a certificate signed by an officer who has been assigned such responsibility. For the client organization and each of its information systems covered by the certification, these documents shall identify the scope of the certification granted and the ISMS standard ISO/IEC 27001 to which the ISMS is certified. In addition, the certificate shall include a reference to the specific version of the Statement of Applicability.

NOTE A change to the Statement of Applicability which does not change the coverage of the controls of the scope of certification need not require an update of the certificate.

8.3 Directory of certified clients

The requirements from ISO/IEC 17021:2011, Clause 8.3 apply.

8.4 Reference to certification and use of marks

The requirements from ISO/IEC 17021:2011, Clause 8.4 apply. In addition, the following ISMS-specific requirements and guidance applies.

8.4.1 IS 8.4 Control of certification marks

The certification body shall exercise proper control over ownership, use and display of its ISMS certification marks. If the certification body confers the right to use a mark to indicate certification of an ISMS, the certification body shall ensure that the client organization uses the specified mark only as authorised in writing by the certification body. The certification body shall not entitle the client organization to use this mark on a product, or in a way that may be interpreted as denoting product conformity.

8.5 Confidentiality

The requirements from ISO/IEC 17021:2011, Clause 8.5 apply. In addition, the following ISMS-specific requirements and guidance applies.

8.5.1 IS 8.5 Access to organizational records

Before the certification audit, the certification body shall ask the client organization to report if any ISMS records cannot be made available for review by the audit team because they contain confidential or sensitive information. The certification body shall determine whether the ISMS can be adequately audited in the absence of these records. If the certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive records, it shall advise the client organization that the certification audit cannot take place until appropriate access arrangements are granted.

8.6 Information exchange between a certification body and its clients

The requirements from ISO/IEC 17021:2011, Clause 8.6 apply.