INTERNATIONAL STANDARD

ISO/IEC 27006

Third edition
2015-10-01

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 27006:2015(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

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.

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).

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

ISO/IEC 27006 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 27006:2011), which has been technically revised.

Introduction

ISO/IEC 17021-1 sets out criteria for bodies operating audit and certification of management systems. If such bodies are to be accredited as complying with ISO/IEC 17021-1 with the objective of auditing and certifying information security management systems (ISMS) in accordance with ISO/IEC 27001:2013, some additional requirements and guidance to ISO/IEC 17021-1 are necessary. These are provided by this International Standard.

The text in this International Standard follows the structure of ISO/IEC 17021-1 and the additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021-1 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 17021-1 and ISO/IEC 27001, are mandatory. The term "should" is used to indicate recommendation.

The primary purpose 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.

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 systems, 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 17021-1 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 documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

ISO/IEC 27000, *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/IEC 17021-1, ISO/IEC 27000 and the following apply.

3.1
certification documents
documents indicating that a client's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system

4 Principles

The principles from ISO/IEC 17021-1, 4 apply.

5 General requirements

5.1 Legal and contractual matters

The requirements of ISO/IEC 17021-1, 5.1 apply.

5.2 Management of impartiality

The requirements of ISO/IEC 17021-1, 5.2 apply. In addition, the following requirements and guidance apply.

5.2.1 IS 5.2 Conflicts of interest

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

a) 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 publicly available, i.e. they shall not provide company-specific advice which contravenes the requirements of b) below;

b) making available or publishing on request information describing the certification body's interpretation of the requirements of the certification audit standards (see 9.1.3.6);

c) 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;

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

e) 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 not provide internal information security reviews of the client's ISMS subject to certification. Furthermore, the certification body shall be independent from the body or bodies (including any individuals) which provide the internal ISMS audit.

5.3 Liability and financing

The requirements of ISO/IEC 17021-1, 5.3 apply.

6 Structural requirements

The requirements of ISO/IEC 17021-1, 6 apply.

7 Resource requirements

7.1 Competence of personnel

The requirements of ISO/IEC 17021-1, 7.1 apply. In addition, the following requirements and guidance apply.

7.1.1 IS 7.1.1 General considerations

7.1.1.1 Generic competence requirements

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

The certification body shall define the competence requirements for each certification function as referenced in Table A.1 of ISO/IEC 17021-1. The certification body shall take into account all the requirements specified in ISO/IEC 17021-1 and 7.1.2 and 7.2.1 of this International Standard that are relevant for the ISMS technical areas as determined by the certification body.

NOTE Annex A provides a summary of the competence requirements for personnel involved in specific certification functions.

7.1.2 IS 7.1.2 Determination of Competence Criteria

7.1.2.1 Competence requirements for ISMS auditing

7.1.2.1.1 General requirements

The certification body shall have criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least:

a) knowledge of information security;

b) technical knowledge of the activity to be audited;

c) knowledge of management systems;

d) knowledge of the principles of auditing;

NOTE Further information on the principles of auditing can be found in ISO 19011.

e) knowledge of ISMS monitoring, measurement, analysis and evaluation.

These above requirements a) to e) apply to all auditors being part of the audit team, with the exception of b), which can be shared among auditors being part of the audit team.

The audit team shall be competent to trace indications of information security incidents in the client's ISMS back to the appropriate elements of the ISMS.

The audit team shall have appropriate work experience of the items above and practical application of these items (this does not mean that an auditor needs a complete range of experience of all areas of information security, but the audit team as a whole shall have enough appreciation and experience to cover the ISMS scope being audited).

7.1.2.1.2 Information security management terminology, principles, practices and techniques

Collectively, all members of the audit team shall have knowledge of:

a) ISMS specific documentation structures, hierarchy and interrelationships;

b) information security management related tools, methods, techniques and their application;

c) information security risk assessment and risk management;

d) processes applicable to ISMS;

e) the current technology where information security may be relevant or an issue.

Every auditor shall fulfil a), c) and d).

7.1.2.1.3 Information security management system standards and normative documents

Auditors involved in ISMS auditing shall have knowledge of:

a) all requirements contained in ISO/IEC 27001.

Collectively, all members of the audit team shall have knowledge of:

b) all controls contained in ISO/IEC 27002 (if determined as necessary also from sector specific standards) and their implementation, categorized as:

   1) information security policies;

   2) organization of information security;

   3) human resource security;

   4) asset management;

   5) access control, including authorization;

   6) cryptography;

   7) physical and environmental security;

   8) operations security, including IT-services;

   9) communications security, including network security management and information transfer;

   10) system acquisition, development and maintenance;

   11) supplier relationships, including outsourced services;

   12) information security incident management;

   13) information security aspects of business continuity management, including redundancies;

   14) compliance, including information security reviews.

7.1.2.1.4 Business management practices

Auditors involved in ISMS auditing shall have knowledge of:

a) industry information security good practices and information security procedures;

b) policies and business requirements for information security;

c) general business management concepts, practices and the inter-relationship between policy, objectives and results;

d) management processes and related terminology.

NOTE These processes also include human resources management, internal and external communication and other relevant support processes.

7.1.2.1.5 Client business sector

Auditors involved in ISMS auditing shall have knowledge of:

a) the legal and regulatory requirements in the particular information security field, geography and jurisdiction(s);

NOTE Knowledge of legal and regulatory requirements does not imply a profound legal background.

b) information security risks related to business sector;

c) generic terminology, processes and technologies related to the client business sector;

d) the relevant business sector practices.

The criteria a) may be shared amongst the audit team.

7.1.2.1.6 Client products, processes and organization

Collectively, auditors involved in ISMS auditing shall have knowledge of:

a) the impact of organization type, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing;

b) complex operations in a broad perspective;

c) legal and regulatory requirements applicable to the product or service.

7.1.2.2 Competence requirements for leading the ISMS audit team

In addition to the requirements in 7.1.2.1, audit team leaders shall fulfil the following requirements, which shall be demonstrated in audits under guidance and supervision:

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

b) demonstration of the capability to communicate effectively, both orally and in writing.

7.1.2.3 Competence requirements for conducting the application review

7.1.2.3.1 Information security management system standards and normative documents

Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of:

a) relevant ISMS standards and other normative documents used in the certification process.

7.1.2.3.2 Client business sector

Personnel conducting the application review to determine the audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of:

a) generic terminology, processes, technologies and risks related to the client business sector.

7.1.2.3.3 Client products, processes and organization

Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of:

a) client products, processes, organization types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing functions.

7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions

7.1.2.4.1 General

The personnel reviewing audit reports and making certification decisions shall have knowledge that enables them to verify the appropriateness of the scope of certification as well as changes to the scope and their impact on the effectiveness of the audit, in particular the continuing validity of the identification of interfaces and dependencies and the associated risks.

Additionally, the personnel reviewing audit reports and making the certification decisions shall have knowledge of:

a) management systems in general;

b) audit processes and procedures;

c) audit principles, practices and techniques.

7.1.2.4.2 Information security management terminology, principles, practices and techniques

The personnel reviewing audit reports and making the certification decisions shall have knowledge of:

a) the items listed in 7.1.2.1.2 a), c) and d);

b) legal and regulatory requirements relevant to information security.

7.1.2.4.3 Information security management system standards and normative documents

Personnel reviewing audit reports and making certification decisions shall have knowledge of:

a) relevant ISMS standards and other normative documents used in the certification process.

7.1.2.4.4 Client business sector

Personnel reviewing audit reports and making certification decisions shall have knowledge of:

a) generic terminology and risks related to the relevant business sector practices.

7.1.2.4.5 Client products, processes and organization

Personnel reviewing audit reports and making certification decisions shall have knowledge of:

a) client products, processes, organization types, size, governance, structure, functions and relationships.

7.2 Personnel involved in the certification activities

The requirements of ISO/IEC 17021-1, 7.2 apply. In addition, the following requirements and guidance apply.

7.2.1 IS 7.2 Demonstration of auditor knowledge and experience

The certification body shall demonstrate that the auditors have knowledge and experience through:

a) recognized ISMS-specific qualifications;

b) registration as auditor where applicable;

c) participation in ISMS training courses and attainment of relevant personal credentials;

d) up to date professional development records;

e) ISMS audits witnessed by another ISMS auditor.

7.2.1.1 Selecting auditors

In addition to 7.1.2.1, the criteria for selecting auditors shall ensure that each auditor:

a) has professional education or training to an equivalent level of university education;

b) has 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) has successfully completed at least five days of training, the scope of which covers ISMS audits and audit management;

d) has 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 ISMS certification audits, including re-certification and surveillance audits, for a total of at least 20 days of which at most 5 days may come from surveillance audits. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting;

e) has relevant and current experience;

f) keeps current knowledge and skills in information security and auditing up to date through continual professional development.

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

7.2.1.2 Selecting auditors for leading the team

In addition to 7.1.2.2 and 7.2.1.1, the criteria for selecting an auditor for leading the team shall ensure that this auditor:

a) has actively participated in all stages of at least three ISMS audits. The participation shall include initial scoping and planning, review of documentation and risk assessment, implementation assessment and formal audit reporting.

7.3 Use of individual external auditors and external technical experts

The requirements of ISO/IEC 17021-1, 7.3 apply. In addition, the following requirements and guidance apply.

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

Technical experts shall work under the supervision of an auditor. The minimum requirements for technical experts are listed in 7.2.1.1.

7.4 Personnel records

The requirements of ISO/IEC 17021-1, 7.4 apply.

7.5 Outsourcing

The requirements of ISO/IEC 17021-1, 7.5 apply.

8 Information requirements

8.1 Public information

The requirements of ISO/IEC 17021-1, 8.1 apply.

8.2 Certification documents

The requirements of ISO/IEC 17021-1, 8.2 apply. In addition, the following requirements and guidance apply.

8.2.1 IS 8.2 ISMS Certification documents

Certification documents shall be signed by an officer who has been assigned such responsibility. The version of the Statement of Applicability shall be included in the certification documents.

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

Identification of the sector-specific standard(s) used may also be included in the certification documents.

8.3 Reference to certification and use of marks

The requirements of ISO/IEC 17021-1, 8.3 apply.

8.4 Confidentiality

The requirements of ISO/IEC 17021-1, 8.4 apply. In addition, the following requirements and guidance apply.

8.4.1 IS 8.4 Access to organizational records

Before the certification audit, the certification body shall ask the client to report if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. The certification body shall determine whether the ISMS can be adequately audited in the absence of such information. If the certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, it shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted.

8.5 Information exchange between a certification body and its clients

The requirements of ISO/IEC 17021-1, 8.5 apply.

9 Process requirements

9.1 Pre-certification activities

9.1.1 Application

The requirements of ISO/IEC 17021-1, 9.1.1 apply. In addition, the following requirements and guidance apply.

9.1.1.1 IS 9.1.1 Application readiness

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

9.1.2 Application review

The requirements of ISO/IEC 17021-1, 9.1.2 apply.

9.1.3 Audit programme

The requirements of ISO/IEC 17021-1, 9.1.3 apply. In addition, the following requirements and guidance apply.

9.1.3.1 IS 9.1.3 General

The audit programme for ISMS audits shall take the determined information security controls into account.

9.1.3.2 IS 9.1.3 Audit Methodology

The certification body's procedures shall not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records. Certification procedures shall focus on establishing that a client's ISMS meets the requirements specified in ISO/IEC 27001 and the policies and objectives of the client.

NOTE Further guidance on auditing is given in ISO/IEC 27007.

9.1.3.3 IS 9.1.3 General preparations for the initial audit

The certification body shall require that a client makes all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security.

At least the following information shall be provided by the client during stage 1 of the certification audit:

a) general information concerning the ISMS and the activities it covers;

b) a copy of the required ISMS documentation specified in ISO/IEC 27001 and, where required, associated documentation.

9.1.3.4 IS 9.1.3 Review periods

The certification body shall not certify an ISMS unless it has been operated through at least one management review and one internal ISMS audit covering the scope of certification.

9.1.3.5 IS 9.1.3 Scope of certification

The audit team shall audit the ISMS of the client covered by the defined scope against all applicable certification requirements. The certification body shall confirm, in the scope of the client ISMS, that clients address the requirements stated in ISO/IEC 27001, 4.3.

Certification bodies shall ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability. The certification body shall verify that there is at least one Statement of Applicability per scope of certification.

Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included

in the client's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations.

9.1.3.6 IS 9.1.3 Certification audit criteria

The criteria against which the ISMS of a client is audited shall be the ISMS standard ISO/IEC 27001. Other documents may be required for certification relevant to the function performed.

9.1.4 Determining audit time

The requirements of ISO/IEC 17021-1, 9.1.4 apply. In addition, the following requirements and guidance apply.

9.1.4.1 IS 9.1.4 Audit time

Certification bodies shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit. The calculation of overall audit time shall include sufficient time for audit reporting.

The certification body shall use Annex B to determine audit time.

NOTE Further guidance and examples on audit time calculation are provided in Annex C.

9.1.5 Multi-site sampling

The requirements of ISO/IEC 17021-1, 9.1.5 apply. In addition, the following requirements and guidance apply.

9.1.5.1 IS 9.1.5 Multiple sites

9.1.5.1.1 Where a client has a number of sites meeting the criteria from a) to c) below, certification bodies may consider using a sample-based approach to multiple-site certification audit:

a) all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review;

b) all sites are included within the client's internal ISMS audit programme;

c) all sites are included within the client's ISMS management review programme.

9.1.5.1.2 The certification body wishing to use a sample-based approach shall have procedures in place to ensure the following:

a) The initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined.

b) A representative number of sites have been sampled by the certification body, taking into account:

   1) the results of internal audits of the head office and the sites;

   2) the results of management review;

   3) variations in the size of the sites;

   4) variations in the business purpose of the sites;

   5) complexity of the information systems at the different sites;

   6) variations in working practices;

7) variations in activities undertaken;

8) variations of design and operation of controls;

9) potential interaction with critical information systems or information systems processing sensitive information;

10) any differing legal requirements;

11) geographical and cultural aspects;

12) risk situation of the sites;

13) information security incidents at the specific sites.

c) A representative sample is selected from all sites within the scope of the client's ISMS; this selection shall be based upon judgmental choice to reflect the factors presented in item b) above as well as a random element.

d) Every site included in the ISMS which is subject to significant risks is audited by the certification body prior to certification.

e) The audit programme has been designed in the light of the above requirements and covers representative samples of the scope of the ISMS certification within the three year period.

f) In the case of a nonconformity being observed, either at the head office or at a single site, the corrective action procedure applies to the head office and all sites covered by the certificate.

The audit shall address the client's head office activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above.

9.1.6 Multiple management systems

The requirements of ISO/IEC 17021-1, 9.1.6 apply. In addition, the following requirements and guidance apply.

9.1.6.1 IS 9.1.6 Integration of ISMS documentation with that for other management systems

The certification body may accept documentation that is combined (e.g. for information security, quality, health and safety and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems.

9.1.6.2 IS 9.1.6 Combining management system audits

The ISMS audit may be combined with audits of other management systems, provided that it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the elements important to an ISMS shall appear clearly and be readily identifiable in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits.

9.2 Planning audits

9.2.1 Determining audit objectives, scope and criteria

The requirements of ISO/IEC 17021-1, 9.2.1 apply. In addition, the following requirements and guidance apply.

9.2.1.1 IS 9.2.1 Audit objectives

The audit objectives shall include the determination of the effectiveness of the management system to ensure that the client, based on the risk assessment, has implemented applicable controls and achieved the established information security objectives.

9.2.2 Audit team selection and assignments

The requirements of ISO/IEC 17021-1, 9.2.2 apply. In addition, the following requirements and guidance apply.

9.2.2.1 IS 9.2.2 Audit team

The audit team shall be formally appointed and provided with the appropriate working documents. The mandate given to the audit team shall be clearly defined and made known to the client.

An audit team may consist of one person provided that the person meets all the criteria set out in 7.1.2.1.

9.2.2.2 IS 9.2.2 Audit team competence

The requirements listed in 7.1.2 apply. For surveillance and special audit activities, only those requirements which are relevant to the scheduled surveillance activity and special audit activity apply.

When selecting and managing the audit team to be appointed for a specific certification audit the certification body shall ensure that the competences 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 may fulfil this function);

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

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

NOTE Appropriate understanding does not imply a profound legal background.

9.2.3 Audit plan

The requirements of ISO/IEC 17021-1, 9.2.3 apply. In addition, the following requirements and guidance apply.

9.2.3.1 IS 9.2.3 General

The audit plan for ISMS audits shall take the determined information security controls into account.

9.2.3.2 IS 9.2.3 Network-assisted audit techniques

The audit plan shall identify the network-assisted auditing techniques that will be utilized during the audit, as appropriate.

Network assisted auditing techniques may include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the ISMS documentation or ISMS processes. The focus of such techniques should be to enhance audit effectiveness and efficiency and should support the integrity of the audit process.

9.2.3.3 IS 9.2.3 Timing of audit

A certification body should agree with the organization to be audited the timing of the audit which will best demonstrate the full scope of the organization. The consideration could include season, month, day/dates and shift as appropriate.

9.3 Initial certification

The requirements of ISO/IEC 17021-1, 9.3 apply. In addition, the following requirements and guidance apply.

9.3.1 IS 9.3.1 Initial certification audit

9.3.1.1 IS 9.3.1.1 Stage 1

In this stage of the audit the certification body shall obtain documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001.

The certification body shall obtain a sufficient understanding of the design of the ISMS in the context of the client's organization, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit. This allows planning for stage 2.

The results of stage 1 shall be documented in a written report. The certification body shall review the stage 1 audit report before deciding on proceeding with stage 2 and for selecting the stage 2 audit team members with the necessary competence.

The certification body shall make the client aware of the further types of information and records that may be required for detailed examination during stage 2.

9.3.1.2 IS 9.3.1.2 Stage 2

9.3.1.2.1 On the basis of findings documented in the stage 1 audit report, the certification body develops an audit plan for the conduct of stage 2. In addition to evaluating the effective implementation of the ISMS, the objectives of stage 2 are:

a) to confirm that the client adheres to its own policies, objectives and procedures.

9.3.1.2.2 To do this, the audit shall focus on the client's:

a) top management leadership and commitment to information security policy and the information security objectives;

b) documentation requirements listed in ISO/IEC 27001;

c) assessment of information security related risks and that the assessments produce consistent, valid and comparable results if repeated;

d) determination of control objectives and controls based on the information security risk assessment and risk treatment processes;

e) information security performance and the effectiveness of the ISMS, evaluating against the information security objectives;

f) correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment and risk treatment process and the information security policy and objectives;

g) implementation of controls (see Annex D), taking into account the external and internal context and related risks, the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives;

h) programmes, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.

9.4 Conducting audits

The requirements of ISO/IEC 17021-1, 9.4 apply. In addition, the following requirements and guidance apply.

9.4.1 IS 9.4 General

The certification body shall have documented procedures for:

a) the initial certification audit of a client's ISMS, in accordance with the provisions of ISO/IEC 17021-1;

b) surveillance and re-certification audits of a client's ISMS in accordance with ISO/IEC 17021-1 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that a client takes corrective action on a timely basis to correct all nonconformities.

9.4.2 IS 9.4 Specific elements of the ISMS audit

The certification body, represented by the audit team, shall:

a) require the client to demonstrate that the assessment of information security related risks is relevant and adequate for the ISMS operation within the ISMS scope;

b) establish whether the client's procedures for the identification, examination and evaluation of information security related risks and the results of their implementation are consistent with the client's policy, objectives and targets.

The certification body shall also establish whether the procedures employed in risk assessment are sound and properly implemented.

9.4.3 IS 9.4 Audit report

9.4.3.1 In addition to the requirements for reporting in ISO/IEC 17021-1, 9.4.8, the audit report shall provide the following information or a reference to it:

a) an account of the audit including a summary of the document review;

b) an account of the certification audit of the client's information security risk analysis;

c) deviations from the audit plan (e.g. more or less time spent on certain scheduled activities);

d) the ISMS' scope.

9.4.3.2 The audit report shall be of sufficient detail to facilitate and support the certification decision. It shall contain:

a) significant audit trails followed and audit methodologies utilized (see 9.1.3.2);

b) observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities);

c) comments on the conformity of the client's ISMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the client.

Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents shall be submitted to the certification body as evidence to support the certification decision. Information about the samples evaluated during the audit shall be included in the audit report, or in other certification documentation.

The report shall consider the adequacy of the internal organization and procedures adopted by the client to give confidence in the ISMS.

In addition to the requirements for reporting in ISO/IEC 17021-1, 9.4.8, the report shall cover:

— a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and IS controls;

— the audit team's recommendation as to whether the client's ISMS should be certified or not, with information to substantiate this recommendation.

9.5 Certification decision

The requirements of ISO/IEC 17021-1, 9.5 apply. In addition, the following requirements and guidance apply.

9.5.1 IS 9.5 Certification decision

The certification decision shall be based, additionally to the requirements of ISO/IEC 17021-1, on the certification recommendation of the audit team as provided in their certification audit report (see 9.4.3).

The persons or committees that take the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation does arise, the certification body shall document and justify the basis for the decision to overturn the recommendation.

Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained.

9.6 Maintaining certification

9.6.1 General

The requirements of ISO/IEC 17021-1, 9.6.1 apply.

9.6.2 Surveillance activities

The requirements of ISO/IEC 17021-1, 9.6.2 apply. In addition, the following requirements and guidance apply.

9.6.2.1 IS 9.6.2 Surveillance activities

9.6.2.1.1 Surveillance audit procedures shall be consistent with those concerning the certification audit of the client's ISMS as described in this International Standard.

The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client's operation and

to confirm continued compliance with certification requirements. Surveillance audit programmes shall cover at least:

a) the system maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and corrective action;

b) communications from external parties as required by the ISMS standard ISO/IEC 27001 and other documents required for certification;

c) changes to the documented system;

d) areas subject to change;

e) selected requirements of ISO/IEC 27001;

f) other selected areas as appropriate.

9.6.2.1.2 As a minimum, every surveillance by the certification body shall review the following:

a) the effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy;

b) the functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;

c) changes to the controls determined, and resulting changes to the SoA;

d) implementation and effectiveness of controls according to the audit programme.

9.6.2.1.3 The certification body shall be able to adapt its surveillance programme to the information security issues related to risks and impacts on the client and justify this programme.

Surveillance audits may be combined with audits of other management systems. The reporting shall clearly indicate the aspects relevant to each management system.

During surveillance audits, certification bodies shall check the records of appeals and complaints brought before the certification body and, where any nonconformity or failure to meet the requirements of certification is revealed, that the client has investigated its own ISMS and procedures and taken appropriate corrective action.

A surveillance report shall contain, in particular, information on clearing of nonconformities revealed previously and the version of the SoA and important changes from the previous audit. As a minimum, the reports arising from surveillance shall build up to cover in totality the requirements of 9.6.2.1.1 and 9.6.2.1.2 above.

9.6.3 Re-certification

The requirements of ISO/IEC 17021-1, 9.6.3 apply. In addition, the following requirements and guidance apply.

9.6.3.1 IS 9.6.3 Re-certification audits

Re-certification audit procedures shall be consistent with those concerning the initial certification audit of the client's ISMS as described in this International Standard.

The time allowed to implement corrective action shall be consistent with the severity of the nonconformity and the associated information security risk.

9.6.4 Special audits

The requirements of ISO/IEC 17021-1, 9.6.4 apply. In addition, the following requirements and guidance apply.

9.6.4.1 IS 9.6.4 Special cases

The activities necessary to perform special audits shall be subject to special provision if a client with a certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification.

9.6.5 Suspending, withdrawing or reducing the scope of certification

The requirements of ISO/IEC 17021-1, 9.6.5 apply.

9.7 Appeals

The requirements of ISO/IEC 17021-1, 9.7 apply.

9.8 Complaints

The requirements of ISO/IEC 17021-1, 9.8 apply. In addition, the following requirements and guidance apply.

9.8.1 IS 9.8 Complaints

Complaints represent a potential incident and an indication to possible nonconformity.

9.9 Client records

The requirements of ISO/IEC 17021-1, 9.9 apply.

10 Management system requirements for certification bodies

10.1 Options

The requirements of ISO/IEC 17021-1, 10.1 apply. In addition, the following requirements and guidance apply.

10.1.1 IS 10.1 ISMS implementation

It is recommended that certification bodies implement an ISMS in accordance with ISO/IEC 27001.

10.2 Option A: General management system requirements

The requirements of ISO/IEC 17021-1, 10.2 apply.

10.3 Option B: Management system requirements in accordance with ISO 9001

The requirements of ISO/IEC 17021-1, 10.3 apply.

Annex A
(informative)

Knowledge and skills for ISMS auditing and certification

A.1 Overview

Table A.1 provides a summary of the knowledge and skills required for ISMS auditing and certification but is informative because it only identifies the areas of knowledge and skills for specific certification functions.

The competence requirements for each function are stated in the main text of this International Standard and this table gives the reference to the specific requirement.

Table A.1 — Knowledge for ISMS auditing and certification

	Certification functions		
	Conducting the application review (Conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time)	Reviewing audit reports and making certification decisions	Auditing and leading the audit team
Knowledge			
Information security management terminology, principles, practices and techniques		7.1.2.4.2	7.1.2.1.2
Information security management system standards/normative documents	7.1.2.3.1	7.1.2.4.3	7.1.2.1.3
Business management practices			7.1.2.1.4
Client business sector	7.1.2.3.2	7.1.2.4.4	7.1.2.1.5
Client products, processes and organization	7.1.2.3.3	7.1.2.4.5	7.1.2.1.6

A.2 General competence considerations

There are several ways by which auditors can prove their knowledge and experience. Knowledge and experience can be evaluated, for example, by using recognized qualifications. Registration records under a personnel certification scheme can also be used to evaluate the required knowledge and experience. The required competence level for the audit team should be established, corresponding with the organization's industry/technological field and complexity of the ISMS.

A.3 Specific knowledge and experience considerations

A.3.1 Typical knowledge related to ISMS

In addition to the requirements in 7.1.2 the following should be considered. Auditors should have knowledge and understanding of the following auditing and ISMS subjects:

— audit programming and planning;

— audit type and methodologies;

— audit risk;

— information security processes analysis;

— continual improvement;

— internal auditing of information security.

Auditors should have knowledge and understanding of the following regulatory requirements:

— intellectual property;

— content, protection and retention of organizational records;

— data protection and privacy;

— regulation of cryptographic controls;

— electronic commerce;

— electronic and digital signatures;

— workplace surveillance;

— telecommunications interception and monitoring of data (e.g. e-mail);

— computer abuse;

— electronic evidence collection;

— penetration testing;

— international and national sector-specific requirements (e.g. banking).

Annex B
(normative)

Audit time

B.1 Introduction

This Annex contains further requirements related to ISO/IEC 17021-1, 9.1. This Annex provides minimum requirements and guidance for a certification body on the development of its own procedures for determining the amount of time required for the certification of client's ISMS scopes of differing sizes and complexity over a broad spectrum of activities.

Certification bodies shall identify the amount of audit time to be spent on initial certification, surveillance and re-certification for each client and certified ISMS. Using this Annex at the audit-planning phase leads to a consistent approach to the determination of appropriate audit time. Additionally, the audit time may be adjusted based on what is found during the course of the audit, especially during stage 1 (e.g. different assessment of the complexity of the ISMS scope, or additional sites to in the scope).

This Annex presents:

— concepts that are used for audit time calculation (B.2);

— requirements for the procedures for determining audit time for the different stages of the audit (B.3 to B.5);

— requirements related to multi-site audits (B.6).

Examples for audit time calculation to illustrate the application of Annex B can be found in Annex C.

A basic assumption of this approach is that a calculation scheme for determining audit time should:

a) consider only substantiated attributes that can be determined;

b) be easy enough to be applied efficiently by certification bodies;

c) be complex enough to enable sufficient distinction.

The determination of the audit time is based on the numbers provided in Table B.1 ("Audit time chart") below and shall consider contributing factors for modification.

B.2 Concepts

B.2.1 Number of persons doing work under the organization's control

The total number of persons doing work under the organization's control for all shifts is the starting point for determination of audit time.

NOTE The term "persons doing work under the organization's control" is referred to as personnel in ISO/IEC 17021-1.

Part-time persons doing work under the organization's control contribute to the number of persons doing work under the organization's control proportionally to the number of hours worked as compared with a full-time person doing work under the organization's control. This determination shall depend upon the number of hours worked as compared with a full-time employee.

B.2.2 Auditor day

"Audit time" as referenced in the chart is stated in terms of "Auditor days" spent on the audit. The basis of the calculation of Annex B is an 8 h working day.

B.2.3 Temporary site

A temporary site is a location other than the sites identified in the certification documents where activities, within the scope of certification, are implemented for a defined period of time. These sites could range from major project management sites to minor service/installation sites. The need to visit such sites and the extent of sampling should be based on an evaluation of the risks of the failure to meet the IS objectives due to a nonconformity originated at the temporary site. The sample of such sites selected should represent the range of the organization's competency needs and service variations having given consideration to sizes and types of activities and the various stages of projects in progress. For general sampling see 9.1.5.1.

B.3 Procedure for determining audit time for initial audit

B.3.1 General

The calculation of audit time shall follow a documented procedure.

B.3.2 Remote audit

If remote auditing techniques such as interactive web-based collaboration, web meetings, teleconferences and/or electronic verification of the organization's processes are utilized to interface with the organization, these activities should be identified in the audit plan (see 9.2.3) and may be considered as partially contributing to the total "on-site audit time".

If the certification body develops an audit plan for which the remote auditing activities represent more than 30 % of the planned on-site audit time, the certification body shall justify the audit plan and obtain specific approval from the accreditation body prior to its implementation.

NOTE On-site audit time refers to the on-site audit time allocated for individual sites. Electronic audits of remote sites are considered to be remote audits, even if the electronic audits are physically carried out on the organization's premises.

B.3.3 Audit time calculation

The audit time chart provided below sets out the starting point for an average number of initial audit days (here and in the following, this number encompasses the days for an initial audit (Stage 1 and Stage 2)), which experience has shown to be appropriate for an ISMS scope with a given number of persons doing work under the organization's control. Experience has also demonstrated that for ISMS scopes of a similar size, some will need more time and some less.

The audit time chart below provides the framework that shall be used for audit planning by identifying a starting point based on the total number of persons doing work under the organization's control for all shifts and adjusting this based on the significant factors applying to the ISMS scope to be audited and attributing to each factor an additive or subtractive weighting to modify the base figure. This Audit time chart shall be used, taking account the contributing factors and restrictions of maximal deviation (see B.3.4 and B.3.5 below). The terms used in this chart are explained in B.2 above and Annex C provides examples of how this can be done.

Table B.1 — Audit time chart

Number of persons doing work under the organization's control	QMS audit time for initial audit (auditor days)	EMS audit time for initial audit (auditor days)	ISMS audit time for initial audit (auditor days)	Additive and subtractive factors	Total audit time
1~10	1.5–2	2.5–3	5	See B.3.4	
11~15	2.5	3.5	6	See B.3.4	
16~25	3	4.5	7	See B.3.4	
26~45	4	5.5	8.5	See B.3.4	
46~65	5	6	10	See B.3.4	
66~85	6	7	11	See B.3.4	
86~125	7	8	12	See B.3.4	
126~175	8	9	13	See B.3.4	
176~275	9	10	14	See B.3.4	
276~425	10	11	15	See B.3.4	
426~625	11	12	16.5	See B.3.4	
626~875	12	13	17.5	See B.3.4	
876~1175	13	15	18.5	See B.3.4	
1176~1550	14	16	19.5	See B.3.4	
1551~2025	15	17	21	See B.3.4	
2026~2675	16	18	22	See B.3.4	
2676~3450	17	19	23	See B.3.4	
3451~4350	18	20	24	See B.3.4	
4351~5450	19	21	25	See B.3.4	
5451~6800	20	23	26	See B.3.4	
6801~8500	21	25	27	See B.3.4	
8501~10700	22	27	28	See B.3.4	
> 10,700	Follow progression above	Follow progression above	Follow progression above	See B.3.4	

B.3.4 Factors for adjustment of audit time

The audit time chart shall not be used in isolation. The time allocated shall also consider the following factors which relate to the complexity of the ISMS and therefore to the effort needed to audit the ISMS:

a) complexity of the ISMS (e.g. criticality of information, risk situation of the ISMS, etc.);

b) the type(s) of business performed within scope of the ISMS;

c) previously demonstrated performance of the ISMS;

d) extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks);

e) extent of outsourcing and third party arrangements used within the scope of the ISMS;

f) extent of information system development;

g) number of sites and number of Disaster Recovery (DR) sites;

h) for surveillance or re-certification audit: The amount and extent of change relevant to the ISMS in accordance with ISO/IEC 17021-1, 8.5.3.

Annex C provides examples how these different factors can be taken into account when calculating audit time.

Additional example factors requiring additional audit time are:

— complicated logistics involving more than one building or location in the scope of the ISMS;

— staff speaking more than one language (requiring interpreter(s) or preventing individual auditors from working independently) or documentation provided in more than one language;

— activities that require visiting temporary sites to confirm the activities of the permanent sites(s) whose management system is subject to certification (see paragraph below next list);

— high number of standards and regulations that apply to the ISMS.

Example factors permitting less audit time are:

— no/low risk product/processes;

— processes involving a single general activity (e.g. service only);

— high percentage of persons doing work under the organization's control performing the same tasks;

— prior knowledge of the organization (for example, if the organization has already been certified to another standard by the same certification body);

— high client preparedness for certification (for example, already certified or recognized by another 3rd party scheme);

— high maturity of the management system in place.

In situations where the certification client or certified organization provides their product(s) or service at temporary sites it is important that evaluations of such sites are incorporated into the certification audit and surveillance programmes.

The above factors shall be considered and the adjustments made for those factors that justify more or less audit time for an effective audit. Additive factors may be off-set by subtractive factors. In all cases where adjustments are made to the time provided in the audit time table sufficient evidence and records shall be maintained to justify the variation.

B.3.5 Limitation of deviation of audit time

In order to ensure effective audits being performed and to ensure reliable and comparable results, the audit time provided in the audit time chart shall not be reduced by more than 30 %.

Appropriate reasons for deviation shall be established and documented.

B.3.6 On-site audit time

It is expected that the time calculated for planning and report writing combined should not typically reduce the total on-site "audit time" to less than 70 % of the time shown in the audit time chart. Where additional time is required for planning and/or report writing, this shall not be justification for reducing on-site audit time. Auditor travel time is not included in this calculation and is additional to the audit time referenced in the chart.

NOTE 70 % is a factor based on experience of ISMS audits.

B.4 Audit time for surveillance audit

For the initial certification audit cycle, surveillance time for a given organization should be proportional to the time spent at initial audit with the total amount of time spent annually on surveillance being

about 1/3 of the time spent on the initial audit. The planned surveillance time should be reviewed from time-to-time to account for changes that affect audit time. The time spent for a surveillance audit shall be increased to allow for audit of changes in the ISMS (such as audit of new or changed controls).

B.5 Audit time for re-certification audit

The total amount of time spent performing the re-certification audit shall depend upon the results of any prior audit as defined in 9.4.3 and ISO/IEC 17021-1, 9.6.3. The amount of time spent at re-certification audit should be proportional to the time that would be spent at initial certification audit of the same organization and should be at least 2/3 of the time that would be required for initial certification audit of the same organization at the time that it is to be audited for re-certification.

B.6 Audit time of multi-site

The number of auditor days per site, including the central office, shall be calculated for each site.

Reductions may be applied to take into account the parts of the audit that are not relevant to the central office or the local sites. Reasons for the justification of such reductions shall be recorded by the certification body.

Annex C
(informative)

Methods for audit time calculations

C.1 General

This Annex provides further guidelines on deriving a formula for calculation of audit time. C.2 gives an example of classification of factors that can be used as a base for calculation of audit time and C.3 provides an example for calculation of audit time.

C.2 Classification of factors for calculating audit time

Table C.1 gives examples for the classification of the main factors for the calculation of audit time, as listed in B.3.4, a) to h). This classification can be used by certification bodies to derive an audit time calculation scheme in line with 9.1.4.1:

Table C.1 — Classification of factors for calculating audit time

	Impact on effort		
	Reduced effort	**Normal effort**	**Increased effort**
Factors (see B.3.4)			
a) complexity of the ISMS: • information security requirements [confidentiality, integrity and availability, (CIA)] • number of critical assets • number of processes and services	• Only little sensitive or confidential information, low availability requirements • Few critical assets (in terms of CIA) • Only one key business process with few interfaces and few business units involved	• Higher availability requirements or some sensitive / confidential information • Some critical assets • 2–3 simple business processes with few interfaces and few business units involved	• Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirements • Many critical assets • More than 2 complex processes with many interfaces and business units involved
b) the type(s) of business performed within scope of the ISMS	• Low risk business without regulatory requirements	• High regulatory requirements	• High risk business with (only) limited regulatory requirements
c) previously demonstrated performance of the ISMS	• Recently certified • Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system	• Recent surveillance audit • Not certified but partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented	• No certification and no recent audits • ISMS is new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution)
d) extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks)	• Highly standardized environment with low diversity (few IT-platforms, servers, operating systems, databases, networks, etc.)	• Standardized but diverse IT platforms, servers, operating systems, databases, networks	• High diversity or complexity of IT (e.g. many different segments of networks, types of servers or databases, number of key applications)
e) extent of outsourcing and third party arrangements used within the scope of the ISMS	• No outsourcing and little dependency on suppliers, or • Well-defined, managed and monitored outsourcing arrangements • Outsourcer has a certified ISMS • Relevant independent assurance reports are available	• Several partly managed outsourcing arrangements	• High dependency on outsourcing or suppliers with large impact on important business activities, or • Unknown amount or extent of outsourcing, or • Several unmanaged outsourcing arrangements

Table C.1 *(continued)*

	Impact on effort		
	Reduced effort	**Normal effort**	**Increased effort**
Factors (see B.3.4)			
f) extent of information system development	• No in-house system development • Use of standardized software platforms	• Use of standardized software platforms with complex configuration/ parameterization • (Highly) customized software • Some development activities (in-house or outsourced)	• Extensive internal software development activities with several ongoing projects for important business purpose
g) number of sites and number of Disaster Recovery (DR) sites	• Low availability requirements and no or one alternative DR site	• Medium or High availability requirements and no or one alternative DR site	• High availability requirements e.g. 24/7 services • Several alternative DR sites • Several Data Centers
h) for surveillance or re-certification audit: The amount and extent of change relevant to the ISMS in accordance with ISO/IEC 17021-1, 8.5.3	• No changes since last re-certification audit	• Minor changes in scope or SoA of ISMS, e.g. some policies, documents, etc. • Minor changes in the factors above	• Major changes in scope or SoA of ISMS, e.g. new processes, new business units, areas, risk assessment management methodology, policies, documentation, risk treatment • Major changes in the factors above

C.3 Example for audit time calculation

The following example illustrates how a certification body may use the factors provided in B.3 to calculate audit time. The calculation of audit time in the example below works in the following way:

Step 1: Determination of factors related to business and organization (other than IT): Identify the suitable grade for each of the categories given in Table C.2 and sum up the results.

Step 2: Determination of factors related to IT environment: Identify the suitable grade for each of the categories given in Table C.3 and sum up the results.

Step 3: Based on the results of step 1 and 2 above, identify the impact of factors on audit time by selecting the appropriate entry in Table C.4.

Step 4: Final calculation: The number of days determined by applying the audit time chart (Table B.1) is multiplied by the factor resulting from Step 3. Where multi-site sampling is utilized, the audit days calculated are increased based on the efforts needed to execute the multi-site sampling plan.

This result is the final number of audit days.

Table C.2 — Factors related to business and organization (other than IT)

Category	Grade
Type(s) of business and regulatory requirements	1. Organization works in non-critical business sectors and non-regulated sectors[a] 2. Organization has customers in critical business sectors [a] 3. Organization works in critical business sectors [a]
Process and tasks	1. Standard processes with standard and repetitive tasks; lots of persons doing work under the organization's control carrying out the same tasks; few products or services 2. Standard but non-repetitive processes, with high number of products or services 3. Complex processes, high number of products and services, many business units included in the scope of certification (ISMS covers highly complex processes or relatively high number or unique activities)
[a] Critical business sectors are sectors that may affect critical public services that will cause risk to health, security, economy, image and government ability to function that may have a very large negative impact to the country.	

Table C.2 *(continued)*

Category	Grade
Level of establishment of the MS	1. ISMS is already well established and/or other management systems are in place 2. Some elements of other management systems are implemented, others not 3. No other management system implemented at all, the ISMS is new and not established
a Critical business sectors are sectors that may affect critical public services that will cause risk to health, security, economy, image and government ability to function that may have a very large negative impact to the country.	

Table C.3 — Factors related to IT environment

Category	Grade
IT infrastructure complexity	1. Few or highly standardized IT platforms, servers, operating systems, databases, networks, etc. 2. Several different IT platforms, servers, operating systems, databases, networks 3. Many different IT platforms, servers, operating systems, databases, networks
Dependency on outsourcing and suppliers, including cloud services	1. Little or no dependency on outsourcing or suppliers 2. Some dependency on outsourcing or suppliers, related to some but not all important business activities 3. High dependency on outsourcing or suppliers, large impact on important business activities
Information System development	1. None or a very limited in-house system/application development 2. Some in-house or outsourced system/application development for some important business purposes 3. Extensive in-house or outsourced system/application development for important business purposes

Table C.4 — Impact of factors on audit time

		IT complexity		
		Low (from 3 to 4)	**Medium (from 5 to 6)**	**High (from 7 to 9)**
Business complexity	**High (from 7 to 9)**	+5 % to +20 %	+10 % to +50 %	+20 % to +100 %
	Medium (from 5 to 6)	-5 % to –10 %	0 %	+10 % to +50 %
	Low (from 3 to 4)	-10 % to –30 %	-5 % to –10 %	+5 % to +20 %

EXAMPLE 1 The organization to be audited has 700 employees, thus according to Table B.1, 17.5 days are required for the initial audit. The organization does not work in a critical business sector, has highly standardized and repetitive tasks and has just established the ISMS. According to Table C.2 this would yield a factor related to business and organization of 1+1+3 = 5. The organization has very few IT-platforms and databases but uses outsourcing extensively. There is no development within the organization or outsourced. According to Table C.3 this would yield a factor related to IT environment of 1+3+1 = 5. Using Table C.4 this would yield no adjustment for the audit time.

EXAMPLE 2 The same organization as in the previous example except that several management systems are already in place and the ISMS is already well established. This would change the calculation according to Table C.2 to 1+1+1 = 3. According to Table C.4 this would yield a reduction of 5 % to 10 % of the audit time, i.e. the audit time would be reduced by 1 day to 1.5 days yielding a total of 16 to 16.5 days.

Annex D
(informative)

Guidance for review of implemented ISO/IEC 27001:2013, Annex A controls

D.1 Purpose

The implementation of controls that were determined as necessary by the client for the ISMS (as per the Statement of Applicability) shall be reviewed during stage 2 of the initial audit and during surveillance or re-certification activities [see 9.3.1.2.2 g)].

The audit evidence that the certification body collects shall be sufficient to draw a conclusion as to whether the controls are effective. How a control is expected to perform may, for example, be specified in procedures or policies of the client.

D.1.1 Audit evidence

The best quality of audit evidence is gathered from observation by the auditor (e.g. that a locked door is locked, people do sign confidentiality agreements, the asset register exists and contains assets observed, system settings are adequate, etc.). Evidence can be gathered from seeing the results of performance of a control (e.g. printouts of access rights given to people signed by the correct authorizing official, records of incident resolution, processing authorities signed by the correct authorizing official, minutes of management (or other) meetings etc.). Evidence can be the result of direct testing (or re-performance) of controls by the auditor, e.g. attempts to perform tasks said to be prohibited by the controls, determination whether software to protect against malicious code is installed and up-to-date on machines, access rights granted (after checking to authorities), etc. Evidence can be gathered by interviewing persons doing work under the organization's control/contractors about processes and controls and determining whether this is factually correct.

D.2 How to use Table D.1

D.2.1 General

Table D.1 provides guidance for the review of the implementation of controls listed in ISO/IEC 27001:2013, Annex A, and the gathering of audit evidence as to their performance during the initial audit and subsequent audits. The Table is not intended to provide guidance for reviewing controls other than those in ISO/IEC 27001:2013, Annex A.

D.2.2 Columns "Organizational control" and "Technical control"

An "X" in the respective column indicates whether the control is an organizational or a technical control. As some controls are both organizational and technical, entries can be in both columns for such controls.

Evidence of the performance of organizational controls can be gathered through review of the records of performance of controls, interviews, observation and physical inspection. Evidence of the performance of technical controls can often be gathered through system testing (see below) or through use of specialized audit/reporting tools.

D.2.3 Column "System testing"

"System testing" means direct review of information systems (e.g. review of system settings or configuration). The auditor's questions can be answered at the system console or by evaluation of the

results of testing tools. If the client has a computer-based tool in use that is known to the auditor, this can be used to support the audit, or the results of an evaluation performed by the client (or their sub-contractors) can be reviewed.

The table contains two categories for the review of technical controls:

— "possible": system testing is possible for the evaluation of control implementation, but may not be necessary in an ISMS audit;

— "recommended": system testing is usually necessary in an ISMS audit.

NOTE Within this Annex "system" denotes "information system" unless indicated otherwise.

D.2.4 Column "Visual inspection"

"Visual inspection" means that these controls usually require a visual inspection at the location to evaluate their effectiveness. This means that it is not sufficient to review the respective documentation on paper or through interviews; the auditor should verify the control at the location where it is implemented.

D.2.5 Column "Audit review guidance"

The "Audit review guidance" column provides possible focus areas for the evaluation of the control, as further guidance for the auditor.

Table D.1 — Classification of controls

Controls in ISO/IEC 27001:2013, Annex A	**Organizational control**	**Technical control**	**System testing**	**Visual inspection**	**Audit review guidance**
A.5 Information security policies					
A.5.1 Management direction for information security					
A.5.1.1 Policies for information security	X				
A.5.1.2 Review of the policies for information security	X				
A.6 Organization of information security					
A.6.1 Internal organization					
A.6.1.1 Information security roles and responsibilities	X				
A.6.1.2 Segregation of duties	X				
A.6.1.3 Contact with authorities	X				
A.6.1.4 Contact with special interest groups	X				
A.6.1.5 Information security in project management	X				
A.6.2 Mobile devices and teleworking					
A.6.2.1 Mobile device policy	X	X	possible		Also check implementation of policy where appropriate
A.6.2.2 Teleworking	X	X	possible		Also check implementation of policy where appropriate
A.7 Human resource security					
A.7.1 Prior to employment					
A.7.1.1 Screening	X				
A.7.1.2 Terms and conditions of employment	X				
A.7.2 During employment					
A.7.2.1 Management responsibilities	X				

Table D.1 *(continued)*

Controls in ISO/IEC 27001:2013, Annex A	**Organizational control**	**Technical control**	**System testing**	**Visual inspection**	**Audit review guidance**
A.7.2.2 Information security awareness, education and training	X				Ask staff if they are aware of specific things they should be aware of
A.7.2.3 Disciplinary process	X				
A.7.3 Termination and change of employment					
A.7.3.1 Termination or change of employment responsibilities	X				
A.8 Asset management					
A.8.1 Responsibility for assets					
A.8.1.1 Inventory of assets	X				Identify the assets
A.8.1.2 Ownership of assets	X				
A.8.1.3 Acceptable use of assets	X				
A.8.1.4 Return of assets	X				
A.8.2 Information classification					
A.8.2.1 Classification of information	X				Also check implementation of policy where appropriate
A.8.2.2 Labelling of information	X				Naming: directories, files, printed reports, recorded media (e.g. tapes, disks, CDs), electronic messages and file transfers
A.8.2.3 Handling of assets	X				
A.8.3 Media handling					
A.8.3.1 Management of removable media	X	X	possible		
A.8.3.2 Disposal of media	X			X	Process for disposal
A.8.3.3 Physical media transfer	X				Physical protection
A.9 Access control					
A.9.1 Business requirements of access control					
A.9.1.1 Access control policy	X				Also check implementation of policy where appropriate
A.9.1.2 Access to networks and network services	X				Also check implementation of policy where appropriate
A.9.2 User access management					
A.9.2.1 User registration and de-registration	X				
A.9.2.2 User access provisioning	X	X	possible		Sample persons doing work under the organization's control/ contractors to authorizations for all access rights to all systems
A.9.2.3 Management of privileged access rights	X	X	possible		Internal transfer of staff
A.9.2.4 Management of secret authentication information of users	X				
A.9.2.5 Review of user access rights	X				
A.9.2.6 Removal or adjustment of access rights	X				
A.9.3 User responsibilities					
A.9.3.1 Use of secret authentication information	X				Verify guidelines/ policy in place for users
A.9.4 System and application access control					

Table D.1 *(continued)*

Controls in ISO/IEC 27001:2013, Annex A	**Organizational control**	**Technical control**	**System testing**	**Visual inspection**	**Audit review guidance**
A.9.4.1 Information access restriction	X	X	recommended		
A.9.4.2 Secure log-on procedures	X	X	recommended		
A.9.4.3 Password management system	X	X	recommended		
A.9.4.4 Use of privileged utility programs	X	X	recommended		
A.9.4.5 Access control to program source code	X	X	recommended		
A.10 Cryptography					
A.10.1 Cryptographic controls					
A.10.1.1 Policy on the use of cryptographic controls	X				Also check implementation of policy where appropriate
A.10.1.2 Key management	X	X	recommended		Also check implementation of policy where appropriate
A.11 Physical and environmental security					
A.11.1 Secure areas					
A.11.1.1 Physical security perimeter	X				
A.11.1.2 Physical entry controls	X	X	possible	X	Archiving of access records
A.11.1.3 Securing offices, rooms and facilities	X			X	
A.11.1.4 Protecting against external and environmental threats	X			X	
A.11.1.5 Working in secure areas	X			X	
A.11.1.6 Delivery and loading areas	X			X	
A.11.2 Equipment					
A.11.2.1 Equipment siting and protection	X			X	
A.11.2.2 Supporting utilities	X	X	possible	X	
A.11.2.3 Cabling security	X			X	
A.11.2.4 Equipment maintenance	X				
A.11.2.5 Removal of assets	X				Record of assets taken offsite
A.11.2.6 Security of equipment and assets off-premises	X	X	possible		Portable device encryption
A.11.2.7 Secure disposal or re-use of equipment	X	X	possible	X	Disk wiping, disk encryption
A.11.2.8 Unattended user equipment	X				Verify guidelines/ policy in place for users
A.11.2.9 Clear desk and clear screen policy	X			X	Also check implementation of policy where appropriate
A.12 Operations security					
A.12.1 Operational procedures and responsibilities					
A.12.1.1Documented operating procedures	X				
A.12.1.2 Change management	X	X	recommended		
A.12.1.3 Capacity management	X	X	possible		
A.12.1.4 Separation of development, testing and operational environments	X	X	possible		
A.12.2 Protection from malware					
A.12.2.1 Controls against malware	X	X	recommended		Configuration and completeness of coverage of malware control software.
A.12.3 Backup					

Table D.1 *(continued)*

Controls in ISO/IEC 27001:2013, Annex A	**Organizational control**	**Technical control**	**System testing**	**Visual inspection**	**Audit review guidance**
A.12.3.1 Information backup	X	X	recommended		Review policy, recovery tests
A.12.4 Logging and monitoring					
A.12.4.1 Event logging	X	X	possible		Risk based selection of events to log
A.12.4.2 Protection of log information	X	X	possible		
A.12.4.3 Administrator and operator logs	X	X	possible		
A.12.4.4 Clock synchronisation		X	possible		
A.12.5 Control of operational software					
A.12.5.1 Installation of software on operational systems	X	X	possible		
A.12.6 Technical vulnerability management					
A.12.6.1 Management of technical vulnerabilities	X	X	recommended		Risk based patch management and hardening of operating systems, databases and applications
A.12.6.2 Restrictions on software installation	X	X	possible		
A.12.7 Information systems audit considerations					
A.12.7.1 Information systems audit controls	X				
A.13 Communications security					
A.13.1 Network security management					
A.13.1.1 Network controls	X	X	possible		Network management
A.13.1.2 Security of network services	X	X	recommended		SLAs, information security provisions of network services (e.g. VPN, network routing and connection controls, configuration of network devices)
A.13.1.3 Segregation in networks	X	X	possible		Network diagrams, network segments (e.g. DMZ) and segregation (e.g. VLAN)
A.13.2 Information transfer					
A.13.2.1 Information transfer policies and procedures	X				Also check implementation of policy where appropriate
A.13.2.2 Agreements on information transfer	X				
A.13.2.3 Electronic messaging	X	X	possible		Confirm sample messages conform to policy/ procedures
A.13.2.4 Confidentiality or nondisclosure agreements	X				Contract review
A.14 System acquisition, development and maintenance					
A.14.1 Security requirements of information systems					
A.14.1.1 Information security requirements analysis and specification	X				
A.14.1.2 Securing application services on public networks	X	X	recommended		Risk based design of application services
A.14.1.3 Protecting application services transactions	X	X	recommended		Confidentiality, integrity, non-repudiation
A.14.2 Security in development and support processes					
A.14.2.1 Secure development policy	X				Also check implementation of policy where appropriate

Table D.1 *(continued)*

Controls in ISO/IEC 27001:2013, Annex A	**Organizational control**	**Technical control**	**System testing**	**Visual inspection**	**Audit review guidance**
A.14.2.2 System change control procedures	X	X	recommended		
A.14.2.3 Technical review of applications after operating platform changes	X				
A.14.2.4 Restrictions on changes to software packages	X				
A.14.2.5 Secure system engineering principles	X				
A.14.2.6 Secure development environment	X	X	possible		
A.14.2.7 Outsourced development	X				
A.14.2.8 System security testing	X				
A.14.2.9 System acceptance testing	X	X	possible		
A.14.3 Test data					
A.14.3.1 Protection of test data	X	X	possible	X	
A.15 Supplier relationships					
A.15.1 Information security in supplier relationships					
A.15.1.1 Information security policy for supplier relationships	X				Also check implementation of policy where appropriate
A.15.1.2 Addressing security within supplier agreements	X				Test some contract conditions
A.15.1.3 Information and communication technology supply chain	X				Test some contract conditions
A.15.2 Supplier service delivery management					
A.15.2.1 Monitoring and review of supplier services	X				
A.15.2.2 Managing changes to supplier services	X				
A.16 Information security incident management					
A.16.1 Management of information security incidents and improvements					
A.16.1.1 Responsibilities and procedures	X				
A.16.1.2 Reporting information security events	X				
A.16.1.3 Reporting information security weaknesses	X				
A.16.1.4 Assessment of and decision on information security events	X				
A.16.1.5 Response to information security incidents	X				
A.16.1.6 Learning from information security incidents	X				
A.16.1.7 Collection of evidence	X				
A.17 Information security aspects of business continuity management					
A.17.1 Information security continuity					Management review minutes
A.17.1.1 Planning information security continuity	X				
A.17.1.2 Implementing information security continuity	X				

Table D.1 *(continued)*

Controls in ISO/IEC 27001:2013, Annex A	**Organizational control**	**Technical control**	**System testing**	**Visual inspection**	**Audit review guidance**
A.17.1.3 Verify, review and evaluate information security continuity	X				
A.17.2 Redundancies					
A.17.2.1 Availability of information processing facilities	X	X	possible		
A.18 Compliance					
A.18.1 Compliance with legal and contractual requirements					
A.18.1.1 Identification of applicable legislation and contractual requirements	X		recommended		
A.18.1.2 Intellectual property rights	X				
A.18.1.3 Protection of records	X	X	recommended		
A.18.1.4 Privacy and protection of personally identifiable information	X				Also check implementation of policy where appropriate
A.18.1.5 Regulation of cryptographic controls	X				
A.18.2 Information security reviews					
A.18.2.1 Independent review of information security	X				Read the reports
A.18.2.2 Compliance with security policies and standards	X				
A.18.2.3 Technical compliance review	X	X			

Bibliography

[1] ISO 19011, *Guidelines for auditing management systems*

[2] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[3] ISO 9001, *Quality management systems — Requirements*

ICS 35.040

Price based on 35 pages