INTERNATIONAL STANDARD

ISO/IEC 27007

Third edition
2020-01

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27007:2020(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27007:2017), which has been technically revised.

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

— the document has been aligned with ISO 19011:2018;

— the Introduction has been reworded and expanded;

— in 5.1, the entire text has been removed;

— in 5.2.2, the former item d) has been removed;

— in 5.3, the entire text has been removed;

— in 5.5.2.2, the former item b) and a paragraph below has been removed;

— in 6.5.2.2, the first paragraph has been removed and the NOTE reworded.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

An information security management system (ISMS) audit can be conducted against a range of audit criteria, separately or in combination, including but not limited to:

— requirements defined in ISO/IEC 27001:2013;

— policies and requirements specified by relevant interested parties;

— statutory and regulatory requirements;

— ISMS processes and controls defined by the organization or other parties;

— management system plan(s) relating to the provision of specific outputs of an ISMS (e.g. plans to address risks and opportunities when establishing ISMS, plans to achieve information security objectives, risk treatment plans, project plans).

This document provides guidance for all sizes and types of organizations and ISMS audits of varying scopes and scales, including those conducted by large audit teams, typically of larger organizations, and those by single auditors, whether in large or small organizations. This guidance should be adapted as appropriate to the scope, complexity and scale of the ISMS audit programme.

This document concentrates on ISMS internal audits (first party) and ISMS audits conducted by organizations on their external providers and other external interested parties (second party). This document can also be useful for ISMS external audits conducted for purposes other than third party management system certification. ISO/IEC 27006 provides requirements for auditing ISMS for third party certification; this document can provide useful additional guidance.

This document is to be used in conjunction with the guidance contained in ISO 19011:2018.

This document follows the structure of ISO 19011:2018.

ISO 19011:2018 provides guidance on the management of audit programmes, the conduct of internal or external audits of management systems, as well as on the competence and evaluation of management system auditors.

Annex A provides guidance for ISMS auditing practices along with requirements of ISO/IEC 27001:2013, Clauses 4 to 10.

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

1 Scope

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

This document is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 19011:2018, *Guidelines for auditing management systems*

ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 19011 and ISO/IEC 27000 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

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

4 Principles of auditing

The principles of auditing of ISO 19011:2018, Clause 4, apply.

5 Managing an audit programme

5.1 General

The guidelines of ISO 19011:2018, 5.1, apply.

5.2 Establishing audit programme objectives

5.2.1 The guidelines of ISO 19011:2018, 5.2, apply. In addition, the guidance in 5.2.2 applies.

5.2.2 ISMS-specific considerations for determining audit[1)] programme objectives can include:

a) identified information security requirements;

b) requirements of ISO/IEC 27001;

c) auditee's level of performance, as reflected in the occurrence of information security events and incidents and effectiveness of the ISMS;

NOTE Further information about performance monitoring, measurement, analysis and evaluation can be found in ISO/IEC 27004.

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

Examples of ISMS-specific audit programme objectives include:

— demonstrate conformity with all relevant legal and contractual requirements and other requirements and their security implications;

— obtain and maintain confidence in the risk management capability of the auditee;

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

5.3 Determining and evaluating audit programme risks and opportunities

5.3.1 The guidelines of ISO 19011:2018, 5.3, apply.

5.3.2 Measures to ensure information security and confidentiality should be determined considering auditees and other relevant party requirements. Other party requirements can include relevant legal and contractual requirements.

5.4 Establishing audit programme

5.4.1 Roles and responsibilities of the individual(s) managing audit programme

The guidelines of ISO 19011:2018, 5.4.1, apply. In addition, the guidance in 5.4.1.2 applies.

5.4.2 Competence of individual(s) managing audit programme

The guidelines of ISO 19011:2018, 5.4.2, apply.

5.4.3 Establishing extent of the audit programme

5.4.3.1 The guidelines of ISO 19011:2018, 5.4.3, apply. In addition, the guidance in 5.4.3.2 applies.

5.4.3.2 The extent of an audit programme can include the following:

a) the size of the ISMS, including:

1) the total number of persons doing work under the organization's control and relationships with interested parties and contractors that are relevant to the ISMS;

2) the number of information systems;

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

3) the number of sites covered by the ISMS;

b) the complexity of the ISMS (including the number and criticality of processes and activities) taking into account differences between sites within the ISMS scope;

c) the significance of the information security risks identified for the ISMS in relation to the business;

d) the significance of the risks and opportunities determined when planning the ISMS;

e) the importance of preserving the confidentiality, integrity and availability of information within the scope of the ISMS;

f) the complexity of the information systems to be audited, including complexity of information technology deployed;

g) the number of similar sites.

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

NOTE Further information about determining audit time can be found in ISO/IEC 27006. Further information on multi-site sampling can be found in ISO/IEC 27006 and mandatory document 1 from the International Accreditation Forum (IAF MD1, see Reference [11]). The information contained in ISO/IEC 27006 and IAF MD 1 only relates to certification audits.

5.4.4 Determining audit programme resources

5.4.4.1 The guidelines of ISO 19011:2018, 5.4.4, apply. In addition, the guidance in 5.4.4.2 applies.

5.4.4.2 In particular, for all significant risks applicable to the auditee and relevant to the audit programme objectives, ISMS auditors should be allocated sufficient time to review the effectiveness of the actions to address information security risks and ISMS related risks and opportunities.

5.5 Implementing audit programme

5.5.1 General

The guidelines of ISO 19011:2018, 5.5.1, apply.

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

5.5.2.1 The guidelines of ISO 19011:2018, 5.5.2, apply. In addition, the guidance in 5.5.2.2 applies.

5.5.2.2 The audit objectives may include the following:

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

b) determination of the extent of conformity of information security controls with the requirements and procedures of the ISMS.

The audit scope should take into account information security risks and relevant risks and opportunities affecting the ISMS of relevant parties, i.e. the audit client and the auditee.

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

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

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

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

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

e) the definition of controls to treat risks appropriately;

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

g) information security requirements provided by a customer;

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

5.5.3 Selecting and determining audit methods

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

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

5.5.4 Selecting audit team members

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

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

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

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

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

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

5.5.6 Managing audit programme results

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

5.5.7 Managing and maintaining audit programme records

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

5.6 Monitoring audit programme

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

5.7 Reviewing and improving audit programme

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

6 Conducting an audit

6.1 General

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

6.2 Initiating audit

6.2.1 General

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

6.2.2 Establishing contact with auditee

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

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

6.2.3 Determining feasibility of audit

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

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

6.3 Preparing audit activities

6.3.1 Performing review of documented information

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

6.3.2 Audit planning

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

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

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

6.3.3 Assigning work to audit team

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

6.3.4 Preparing documented information for audit

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

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

6.4 Conducting audit activities

6.4.1 General

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

6.4.2 Assigning roles and responsibilities of guides and observers

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

6.4.3 Conducting opening meeting

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

6.4.4 Communicating during audit

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

6.4.5 Audit information availability and access

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

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

6.4.6 Reviewing document information while conducting audit

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

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

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

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

6.4.7 Collecting and verifying information

6.4.7.1 The guidelines of ISO 19011:2018, 6.4.7, apply. In addition, the guidance in 6.4.7.2 applies.

6.4.7.2 Possible methods to collect relevant information during the audit include:

a) review of documented information (including computer logs and configuration data);

b) visit of information processing facilities;

c) observation of ISMS processes and related controls;

d) use of automated audit tools.

NOTE 1 Annex A provides guidance on how to audit the ISMS processes.

NOTE 2 ISO/IEC TS 27008 provides additional guidance on how to assess information security controls.

ISMS audit team members should ensure appropriate handling of all information received from auditees in accordance with the agreement among the audit client, audit team and the auditee.

6.4.8 Generating audit findings

The guidelines of ISO 19011:2018, 6.4.8, apply.

6.4.9 Determining audit conclusions

The guidelines of ISO 19011:2018, 6.4.9, apply.

6.4.10 Conducting closing meeting

The guidelines of ISO 19011:2018, 6.4.10, apply.

6.5 Preparing and distributing audit report

6.5.1 Preparing audit report

The guidelines of ISO 19011:2018, 6.5.1, apply.

6.5.2 Distributing audit report

6.5.2.1 The guidelines of ISO 19011:2018, 6.5.2, apply. In addition, the guidance in 6.5.2.2 applies.

6.5.2.2 NOTE

NOTE When using electronic means for distribution of the audit report, appropriate encryption is a possible measure to ensure confidentially requirements.

6.6 Completing audit

The guidelines of ISO 19011:2018, 6.6, apply.

6.7 Conducting audit follow-up

The guidelines of ISO 19011:2018, 6.7, apply.

7 Competence and evaluation of auditors

7.1 General

The guidelines of ISO 19011:2018, 7.1, apply.

7.2 Determining auditor competence

7.2.1 General

7.2.1.1 The guidelines of ISO 19011:2018, 7.2.1, apply. In addition, the guidance in 7.2.1.2 applies.

7.2.1.2 In deciding the appropriate knowledge and skills of an ISMS auditor, the following should be taken into consideration:

a) complexity of the ISMS (e.g. criticality of information systems within the ISMS, risk assessment results of the ISMS);

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

c) extent and diversity of technology utilized in the implementation of the various components of the ISMS (such as the implemented controls, documented information and/or process control, technological platforms and solutions involved, etc.);

d) previously demonstrated performance of the ISMS;

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

f) the standards, legal requirements and other requirements relevant to the audit programme.

7.2.2 Personal behaviour

The guidelines of ISO 19011:2018, 7.2.2, apply.

7.2.3 Knowledge and skills

7.2.3.1 General

The guidelines of ISO 19011:2018, 7.2.3.1, apply.

7.2.3.2 Generic knowledge and skills of management system auditors

The guidelines of ISO 19011:2018, 7.2.3.2, apply.

7.2.3.3 Discipline and sector specific competence of auditors

7.2.3.3.1 The guidelines of ISO 19011:2018, 7.2.3.3, apply. In addition, the guidance in 7.2.3.3.2 applies.

7.2.3.3.2 ISMS auditors should also be able to understand the relevant business requirements.

7.2.3.4 Generic competence of audit team leader

The guidelines of ISO 19011:2018, 7.2.3.4, apply.

7.2.3.5 Knowledge and skills for auditing multiple disciplines

The guidelines of ISO 19011:2018, 7.2.3.5, apply.

7.2.4 Achieving auditor competence

7.2.4.1 The guidelines of ISO 19011:2018, 7.2.4, apply. In addition, the guidance in 7.2.4.2 applies.

7.2.4.2 ISMS auditors should have knowledge and skills in information technology and information security, demonstrated for example through relevant certifications (e.g. accredited to ISO/IEC 17024). Individual ISMS auditors work experience should also contribute to the development of their knowledge and skills in the ISMS field.

NOTE Further information about certification for ISMS auditors can be found in ISO/IEC 27006.

7.2.5 Achieving audit team leader competence

The guidelines of ISO 19011:2018, 7.2.5, apply.

7.3 Establishing auditor evaluation criteria

The guidelines of ISO 19011:2018, 7.3, apply.

7.4 Selecting appropriate auditor evaluation method

The guidelines of ISO 19011:2018, 7.4, apply.

7.5 Conducting auditor evaluation

The guidelines of ISO 19011:2018, 7.5, apply.

7.6 Maintaining and improving auditor competence

The guidelines of ISO 19011:2018, 7.6, apply.

Annex A
(informative)

Guidance for ISMS auditing practice

A.1 Overview

This annex provides generic guidance on how to audit an ISMS, for which an organization claims conformance to ISO/IEC 27001. As this guidance is intended to apply to all such ISMS audits, irrespective of the size or nature of the organization involved, this guidance is generic. The guidance is intended to be used by auditors performing ISMS auditing, whether internal or external.

NOTE ISO/IEC 27003 gives guidance on implementing and operating an ISMS according to ISO/IEC 27001.

A.2 General

A.2.1 Audit objectives, scope, criteria and audit evidence

During audit activities, information relevant to the audit objectives, scope and criteria, including information relating to interfaces between functions, activities and processes, should be obtained by means of appropriate sampling and should be verified. Only information that is verifiable should be accepted as audit evidence. Audit evidence leading to audit findings should be recorded.

Methods of obtaining information include the following:

— interviews;

— observations;

— review of documents, including records.

A.2.2 Strategy for auditing an ISMS

There are some ISO/IEC 27001:2013 subclauses that are closely linked and in practice are often best dealt with at the same time in conducting the audit. See Table A.2 for examples.

Examples are ISO/IEC 27001:2013:6.1.3 and 8.3 and 6.2, 5.1, 5.2, 5.3, 7.1, 7.4, 7.5, 9.1, 9.3 and 10.2 and it makes sense to audit these subclauses with those linked and related subclauses.

ISO/IEC 27001:2013, 7.5, presents the requirements concerning documented information. As explained in Table A.2, A.4.5, each time auditors examine an item of documented information, it offers the opportunity to confirm conformity with the requirements of ISO/IEC 27001:2013, 7.5. The guidance on how to do this is located in Table A.2, A.4.5. The requirements regarding documented information are not repeated for each occurrence of "documented information" in the table.

A.2.3 Audit and documented information

Audit activities can involve documented information, namely:

a) requirement statements of documented information in ISO/IEC 27001 can be used as audit criteria;

b) documented information required by ISO/IEC 27001:2013, 7.5.1 b);

c) documented information determined by the organization as being necessary for the effectiveness of the ISMS of ISO/IEC 27001:2013, 7.5.1 c).

There can be audit evidence other than A.2.3 b), which auditors will obtain through interview, observations and review of documents, including records.

Detailed discussion of documented information concerning ISO/IEC 27001 can be found in A.3.

A.3 Guidance on ISO/IEC 27001 requirements for documented information

A.3.1 Rationale

Auditors should take care when requesting documented information as evidence of conformity.

There are:

a) 16 explicit requirements for documented information, including the Statement of Applicability, as listed in Table A.1;

b) further requirements are requirements for which:

   1) it would be reasonable to expect that evidence of conformance will be found in the above-mentioned documented information;

   2) there is no explicit or implicit requirement for documented information.

Table A.1 — Requirements for documented information in ISO/IEC 27001

Requirement for documented information concerning	Subclause in ISO/IEC 27001:2013
Scope of the ISMS	4.3
Information security policy	5.2
Information security risk assessment process	6.1.2
Information security risk treatment process	6.1.3
Statement of Applicability	6.1.3 d)
Information security objectives	6.2
Evidence of competence	7.2 d)
Documented information determined by the organization as being necessary for the effectiveness of the ISMS	7.5.1 b)
Operational planning and control	8.1
Results of the information security risk assessments	8.2
Results of the information security risk treatment	8.3
Evidence of the monitoring and measurement results	9.1
Evidence of the audit programme(s) and the audit results	9.2 g)
Evidence of the results of management reviews	9.3
Evidence of the nature of the nonconformities and any subsequent actions taken	10.1 f)
Evidence of the results of any corrective action	10.1 g)

NOTE The definition of an audit states that it is a documented process and hence, an auditor can expect the requirement of ISO/IEC 27001:2013, 9.2 to result in an audit process being documented.

A.3.2 Example of implicit requirement for documented information

As an example of A.3.1 b) 1), consider ISO/IEC 27001:2013, 6.1.2, which requires organizations to "retain documented information about the information security risk assessment process". The preceding requirements [ISO/IEC 27001:2013, 6.1.2 a) to e)] all concern that risk assessment process. It is therefore reasonable to expect that evidence of conformance to these requirements will be found in the required documented information concerning the risk assessment process.

A.3.3 Example where there is no explicit or implicit requirement for documented information

As an example of A.3.1 b) 2), consider ISO/IEC 27001:2013, 4.1.1. There is no requirement for documented information concerning external and internal issues. Auditors should not therefore demand to see it. Nevertheless, failure of the organization to demonstrate that it has determined these issues would constitute a nonconformity against ISO/IEC 27001:2013, 4.1.1. The onus, however, is on the organization to determine how it chooses to demonstrate conformance. It can be that top management can explain it (i.e. someone knows); it can be that there are minutes of a meeting at which the subject was discussed; it can be evidenced in documented information that is under formal configuration management or it can be evidenced in some other way. Indeed, it is likely that evidence will be scattered across the documented information of the ISMS. For example, the purpose of ISO/IEC 27001:2013, 4.1.1, is to assist the organization in understanding the context of its ISMS. That context prevails throughout the ISMS, particularly in the determination of scope and policy and in the performance of the risk assessment and risk treatment processes. If the organization has fulfilled the requirements of ISO/IEC 27001:2013, 4.1.1, it likely that its knowledge of external and internal issues will be used in these other areas of the ISMS, its use will be consistent and there will likely be evidence of conformance in the documented information concerning these other areas.

A.4 The Statement of Applicability

The Statement of Applicability (SoA) is another area which requires care. The SoA should contain all necessary controls, i.e. the controls that the organization has, as a result of its risk treatment process [ISO/IEC 27001:2013, 6.1.3 c)], determined as being necessary for the modification of information security risk in order to meet its risk acceptance criteria. All necessary controls are the organization's own requirements.

Necessary controls can be ISO/IEC 27001:2013, Annex A, controls, but they are not mandatory. They can be controls taken from other standards (e.g. ISO/IEC 27017) or other sources, or they can have been specially designed by the organization.

In some cases, the organization uses a control that is a variation of an ISO/IEC 27001:2013, Annex A, control and excludes the original ISO/IEC 27001:2013, Annex A, control, the rationale for exclusion being that it has been replaced by the organization's variation of the control. Alternatively, the variation can incorporate the ISO/IEC 27001:2013, Annex A, control and hence, it would not be excluded.

Auditors should look for conformance with the organization's specification of its necessary controls, not with the specification given in ISO/IEC 27001:2013, Annex A. If the organization's specification requires a documented procedure, then this forms part of the organization's conformance to ISO/IEC 27001:2013, 7.5.1 b). If it does not, auditors should not demand to see it. Auditors should note, however, the requirement [ISO/IEC 27001:2013, 8.1)] that the organization should "keep documented information to the extent necessary to have confidence that the processes have been carried out as planned". Since ISO/IEC 27001:2013, 8.1 refers to ISO/IEC 27001:2013, 6.1, the organization's risk treatments plan and therefore its necessary controls, are within the scope of this requirement for documented information.

When auditing the selection of controls, it is better to audit against the information security risk treatment plan(s) [as stated in ISO/IEC 27001:2013, 6.1.3 e)] rather than the individual necessary controls as listed in the Statement of Applicability. This is because the information security risk treatment plan(s) are likely to specify the interaction between necessary controls, which is a consideration that can be missed if only the Statement of Applicability was used.

A.5 Other documented information

The focus of ISO/IEC 27001 is on results. Of the 16 explicit requirements for documented information (see Table A.1), only three concern specifications (the information security risk assessment process, the information security risk treatment process and the audit programme). However, this does not prevent an organization from having documented procedures. Such supporting documentation falls within

scope of ISO/IEC 27001:2013, 7.5.1 b) (documented information determined by the organization as being necessary for the effectiveness of its ISMS). It thereby becomes a requirement of an organization and as such, should be within the scope of an audit.

A.6 Notes

The required information can be part of a webpage or presented to the reader as the results of a database query. Moreover, with the exception of the Statement of Applicability, ISO/IEC 27001 does not give names to documents. Thus, it is possible that the documented information concerning the information security policy is not in a document or webpage called "Information Security Policy". Organizations are entitled to call the information security policy something else. The person(s) with the responsibility and authority for ensuring that the information security management system conforms to the requirements of ISO/IEC 27001:2013, 5.3 a), are the same, should know the relationship between the documented information requirements mandated by ISO/IEC 27001 and their documented information.

A.7 Guidance for auditing an ISMS

Table A.2 lists the following information:

— first row: the number and name of the corresponding ISO/IEC 27001:2013 subclause;

— second row: related clauses (refer to A.2.2 for information on how to use this row);

— third row: relevant definitions of ISO/IEC 27000:2018 for the corresponding ISO/IEC 27001:2013 subclause;

— fourth row: "Audit evidence" possible sources for information on the corresponding ISO/IEC 27001:2013 subclause;

— fifth row: "Audit practice guide" guidance for auditing (refer to A.3);

— sixth row: "Supporting documents" references to further documents which can be helpful for auditing against the corresponding ISO/IEC 27001:2013 subclause.

Table A.2 — Auditing guidelines for ISO/IEC 27001

A.1 Context of the organization (ISO/IEC 27001:2013, Clause 4)	
A.1.1 Understanding the organization and its context (ISO/IEC 27001:2013, 4.1)	
Related ISO/IEC 27001 subclauses	ISO/IEC 27001:2013, 6.1, 9.3
Relevant ISO/IEC 27000 definitions	External context, information security, internal context, management system, organization
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) the important issues that can affect, either positively or negatively, the ISMS; b) the organization; c) the purpose of the organization; d) the intended outcome of the ISMS. Possible sources of the important issues can include:

Table A.2 *(continued)*

	a) environmental characteristics or conditions related to climate, pollution, resource availability, and biodiversity, and the effect these conditions can have on the organization's ability to achieve its objectives; b) the external cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive context, whether international, national, regional or local; c) characteristics or conditions of the organization, such as organizational governance, information flows and decision-making processes; — organizational policies, objectives, and the strategies that are in place to achieve them; — the organization's culture; — standards, guidelines and models adopted by the organization; — the life cycle of the organization's products and services; — information systems, processes, science and technology underlying information security management; d) trends of audits and risk assessment.
Audit practice guide	Auditors should confirm that the organization: a) has a high-level (e.g. strategic) understanding of the important issues that can affect, either positively or negatively, the ISMS; b) knows the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS. NOTE 1 The requirement in ISO/IEC 27001:2013, 4.3 is to "consider the external and internal issues referred to in ISO/IEC 27001:2013, 4.1". An organization can take into consideration something that not necessarily appears in the output. Auditors should also confirm that the intended outcomes include preservation of the confidentiality, integrity and availability of information by applying a risk management process and that risks are adequately managed. Auditors should also verify that the issues include the important topics for the organization, problems for debate and discussion, or changing circumstances and also be verified that the knowledge gained is used to guide the organization's efforts to plan, implement and operate the management system.
Supporting documents	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.1
A.1.2 Understanding the needs and expectations of interested parties (ISO/IEC 27001:2013, 4.2)	
Related ISO/IEC 27001 subclauses	ISO/IEC 27001:2013, 4.1, 4.3
Relevant ISO/IEC 27000 definitions	Interested party
Audit evidence	Audit evidence can be obtained through documented information or other information about: a) the interested parties; b) the needs and expectations of relevant interested parties that are applicable to the ISMS and ISO/IEC 27001. NOTE 2 Potential interested parties can include: a) legal and regulatory authorities (local, regional, state/provincial, national or international);

Table A.2 *(continued)*

	b) parent organizations; c) customers; d) trade and professional associations; e) community groups; f) non-governmental organizations; g) suppliers; h) neighbours; i) members of the organization and others working on behalf of the organization; j) information security experts. NOTE 3 Interested party requirements can include: a) laws; b) permits, licenses or other forms of authorization; c) orders issued by regulatory agencies; d) judgments of courts or administrative tribunals; e) treaties, conventions and protocols; f) relevant industry codes and standards; g) contracts which have been entered into; h) agreements with community groups or non-governmental organizations; i) agreements with public authorities and customers; j) organizational requirements; k) voluntary principles or codes of practice; l) voluntary labelling or environmental commitments; m) obligations arising under contractual arrangements with the organization; n) information and communication exchange. NOTE 4 Interested parties can have different interests, which can be wholly aligned, partially aligned or opposed to the organization's business objectives. An example of where an interested party has interests that are opposed to the organization's objectives is the hacker. The hacker requires the organization to have weak security. The organization should take account of this interested party requirement by having the complete opposite, i.e. strong security. Auditors should be aware that the ISMS considers all internal and external risk sources. Therefore, the organization's understanding of interested parties that are opposed to the organization and their requirements is highly relevant.
Audit practice guide	Auditors should confirm that the organization has a high-level (e.g. strategic) understanding of the needs and expectations of relevant interested parties that are applicable to the ISMS and ISO/IEC 27001. Auditors should verify that the organization has identified the interested party requirements that it decides to voluntarily adopt or enter into an agreement or contract, as well as the needs and expectations that are mandatory because they have been incorporated into laws, regulations, permits and licenses by governmental or court action. It is noted that not all interested party requirements are requirements of the organization and some are not applicable to the organization or relevant to the ISMS. Some interested party needs (e.g. those of a hacker) will be contrary to the purpose of the ISMS and the organization would be expected to ensure through appropriate information security controls that such needs and expectations are not satisfied. Auditors can also confirm that there are interested parties that perceive themselves to be affected by the ISMS and if there are so, they make it known to the organization. Auditors can also verify that the organization uses the knowledge gained to guide its efforts to plan, implement and operate the ISMS.

Table A.2 *(continued)*

Supporting documents	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.2
A.1.3 Determining the scope of the information security management system (ISO/IEC 27001:2013, 4.3)	
Related ISO/IEC 27001 subclauses	ISO/IEC 27001:2013, 4.1, 4.2
Relevant ISO/IEC 27000 definitions	Outsource
Audit evidence	Audit evidence can be obtained through documented information or other information of: — the scope of the organization's management system (as defined by ISO/IEC 27001:2013, 4.3); — the scope of an organization's certification, if applicable; — the Statement of Applicability. NOTE 5 The scope of an organization's certification is not necessarily the same as the scope of its ISMS. In general, the scope of certification will be confined to the ISMS organization.
Audit practice guide	Auditors should confirm that the organization establishes the physical, informational, legal and organizational boundaries to which the ISMS is applied, at its own will and chooses to implement ISO/IEC 27001 within the entire organization or as a specific unit or particular function(s) within an organization. Auditors should verify that the organization's understanding of its context (ISO/IEC 27001:2013, 4.1), the requirements of relevant interested parties (ISO/IEC 27001:2013, 4.2) and interfaces and dependencies between activities performed by the organization and those that are performed by other organizations [ISO/IEC 27001:2013,4.3 c)], have been adequately considered when establishing the scope of the ISMS. Auditors should further confirm that the organization's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the ISMS scope, to the extent applicable to the audit scope. Auditors should verify that there is at least one Statement of Applicability per scope and that all the controls determined in the risk management process are included in the Statement(s) of Applicability. These controls are the necessary controls referred to in ISO/IEC 27001:2013, 6.1.3 b) and are not necessarily ISO/IEC 27001:2013, Annex A controls. They may include sector-specific controls and controls that are designed by the organization or identified from any source. Auditors should also confirm that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to be audited and are included in the organization'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. It should be verified that documentation of the scope is created and controlled in accordance with the requirements of documented information (ISO/IEC 27001:2013, 7.5).
Supporting documents	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.3 ISO/IEC 27006:2015, 8.2, 9.1.3.5 (IS 9.1.3 Scope of certification) ISO/IEC 17021-1:2015, 8.2.2
A.1.4 Information security management system (ISO/IEC 27001:2013, 4.4)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 6.1.1, 6.1.2, 6.1.3, 8.1, 8.2, 8.3
Relevant ISO/IEC 27000 definitions	Continual improvement, information security, management system

Table A.2 *(continued)*

Audit evidence	Audit evidence can be obtained through documented information or other information on the processes required to be established in ISO/IEC 27001, which include: a) processes for management system (ISO/IEC 27001:2013, 4.4); b) operational planning and control processes, including outsourced processes (ISO/IEC 27001:2013, 8.1); c) processes to address risks and opportunities when planning the ISMS, including the information security risk assessment processes (ISO/IEC 27001:2013, 6.1.2 and/or 8.1.2) and the information security risk treatment processes (ISO/IEC 27001:2013, 6.1.3 and/or 8.1.3); d) processes to achieve information security objectives.
Audit practice guide	Auditors should confirm that the organization creates the "necessary but sufficient" set of processes and controls that, together, form an effective management system in conformance to ISO/IEC 27001 and establishes the ISMS of the set of those interrelated or interacting elements. Auditors also should confirm that the organization, in its existing capacity, retains authority, accountability and autonomy, to decide how it will fulfil the ISMS requirements, including the level of detail and extent to which it will integrate the ISMS requirements into its business.
Supporting documents	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.4
A.2 Leadership (ISO/IEC 27001:2013, Clause 5)	
A.2.1 Leadership and commitment (ISO/IEC 27001:2013, 5.1)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 4.1, 4.2, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.1, 7.4, 8.1, 9.3, 10.2
Relevant ISO/IEC 27000 definitions	Information security, top management
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) the information security policy [ISO/IEC 27001:2013, 5.1 a)]; b) the information security objectives [ISO/IEC 27001:2013, 5.1 a)]; c) the organization's processes; d) results of management reviews [ISO/IEC 27001:2013, 5.1 c), e) and g)]; e) evaluation of resource need; f) communication of the importance of effective information security management and of conforming to the information security management system requirements. Evidence can also be obtained through interviews with top management. The results of management reviews can also provide audit evidence with subclauses other than ISO/IEC 27001:2013, 5.1 c), e) and g).
Audit practice guide	Auditors should confirm the visible support, involvement and commitment of the organization's top management which is important to the successful implementation of ISO/IEC 27001. Auditors should also verify that: a) top management delegated tasks are identified; b) top management remains accountable for the satisfactory completion of activities assigned to the organization; c) top management ensures that the information security policy and objectives are established and they are aligned with the strategic direction of the overall organization; d) top management communicates the importance of effective information security management and of conforming to the ISMS requirements;

Table A.2 *(continued)*

	e) top management ensures that the ISMS achieves its intended outcome(s) by supporting the implementation of all information security management processes and in particular, through requesting and reviewing reports on the status and effectiveness of the ISMS [see ISO/IEC 27001:2013, 5.3 b)]; f) top management directs and supports people in the organization directly involved with information security and the ISMS; g) top management ensures the integration of the ISMS requirements into the organization's processes; h) top management ensures the availability of resources for having an effective ISMS; i) top management assesses resource needs during management reviews and set objectives for continual improvement and for monitoring effectiveness of planned activities; j) top management creates a culture and environment that encourages people to work actively towards implementing the requirements of the ISMS and seeking to achieve the information security objectives.
Supporting documents	ISO 31000:2018, 4.2 ISO/IEC 27003:2017, 5.1
A.2.2 Policy (ISO/IEC 27001:2013, 5.2)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 6.2, 7.4
Relevant ISO/IEC 27000 definitions	Information security, policy
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) information security policy (ISO/IEC 27001:2013, 5.1); b) information security objectives [ISO/IEC 27001:2013, 5.2 b) and ISO/IEC 27001:2013, 6.2].
Audit practice guide	Auditors should confirm that: a) the information security policy specifies the high level organizational commitments as required by ISO/IEC 27001, taking into account the organization's purpose; b) the information security policy is either used to frame or build the information security objectives which the organization sets for itself, or are stated explicitly as part of the information security policy; c) documented information of the information security policy is created and controlled in accordance with the requirements of documented information (ISO/IEC 27001:2013, 7.5); d) the information security policy is communicated internally, in accordance with the requirements of the communication clause (ISO/IEC 27001:2013, 7.4); e) the information security policy also is made available to other interested parties as appropriate. With the information security policy containing a commitment to satisfy applicable requirements, in particular, relevant laws and regulations, the ISMS should not be considered out of conformance so long as it results in the prompt detection and corrective action of the system deficiencies that contributed to the instance(s) of nonconformity.
Supporting documents	ISO 31000:2018, 4.3.2 ISO/IEC 27003:2017, 5.2

Table A.2 *(continued)*

A.2.3 Organizational roles, responsibilities and authorities (ISO/IEC 27001:2013, 5.3)	
Related ISO/ IEC 27001 clauses	ISO/IEC 27001:2013, 7.4, 9.2, 9.3
Relevant ISO/IEC 27000 definitions	Information security, organization, top management
Audit evidence	Considering ISO/IEC 27001:2013, 7.5.1 b), audit evidence can be obtained through documented information or other information on: a) the organizational roles; b) the job description of persons doing work under its control that can have impact on the organization's information security performance; c) the implementation of internal audit programme and the audit results; d) the ISMS scope and structure of the organization. In addition, there can be further audit evidence obtained through documented information or other information on the results of management reviews.
Audit practice guide	Auditors should confirm through review of documented information and/or interview that: a) responsibilities and authorities for the implementation of the ISMS requirements are assigned to relevant roles within the organization; b) top management is accountable for these responsibilities and authorities being assigned and communicated to the respective persons performing those roles; c) the responsibilities and authorities are communicated in accordance with the requirements of the communication clause (ISO/IEC 27001:2013, 7.4); d) demonstration of conformance to the requirements of ISO/IEC 27001 is conducted in accordance with the requirements of the internal audit (ISO/IEC 27001:2013, 9.2); e) performance reporting is conducted in accordance with the requirements of management review (ISO/IEC 27001:2013, 9.3). Auditors should verify that responsible individuals have sufficient access to top management to keep management informed of the status and performance of the ISMS. NOTE 6 The role of ensuring that the management system conforms to the requirements of ISO/IEC 27001 can be assigned to an individual, shared by several individuals or assigned to a team.
Supporting documents	ISO 31000:2018, 4.3.3 ISO/IEC 27003:2017, 5.3
A.3 Planning (ISO/IEC 27001:2013, Clause 6)	
A.3.1 Actions to address risks and opportunities (ISO/IEC 27001:2013, 6.1)	
A.3.1.1 General (ISO/IEC 27001:2013, 6.1.1)	
Related ISO/ IEC 27001 clauses	ISO/IEC 27001:2013, 4.1, 4.2, 8.1, 9, 10.2
Relevant ISO/IEC 27000 definitions	Information security, risk, risk management
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS [ISO/IEC 27001:2013, 6.1.1, 7.5.1 b) and 8.1)]; b) the information security risk assessment process (ISO/IEC 27001:2013, 6.1.2); c) the results of the information security risk assessments (ISO/IEC 27001:2013, 8.2); d) the information security risk treatment process (ISO/IEC 27001:2013, 6.1.3); e) the results of the information security risk treatment (ISO/IEC 27001:2013, 8.3);

Table A.2 *(continued)*

	f) the results of monitoring and measurements (ISO/IEC 27001:2013, 9.1); g) the internal audit programme(s) and the results of the internal audit (ISO/IEC 27001:2013, 9.2); h) the results of management reviews (ISO/IEC 27001:2013, 9.3); i) context of the organization (ISO/IEC 27001:2013, 4); j) information security objectives (ISO/IEC 27001:2013, 6.2).
Audit practice guide	Auditors should confirm that the planning: a) is being performed at a level appropriate to establishing the ISMS; b) includes the consideration of the issues relevant to the organization's context identified in (ISO/IEC 27001:2013, 4.1) and the organization's applicable requirements identified in (ISO/IEC 27001:2013, 4.3) in order to address any negative or positive consequence related to ISO/IEC 27001:2013, 6.1.1 a) to c); c) has anticipated potential scenarios and consequences and as such being preventive in addressing undesired effects before they occur; d) addresses the intended outcomes [ISO/IEC 27001:2013, 6.1.1 a)] determined by the organization that include preserving the confidentiality, integrity and availability of information by applying a risk management process; e) includes determining how to incorporate the actions deemed necessary or beneficial into the ISMS, either through objective setting (ISO/IEC 27001:2013, 6.2), operational control (ISO/IEC 27001:2013, 8.1) or other specific clauses of ISO/IEC 27001, e.g. resource provisions (ISO/IEC 27001:2013, 7.1), competence (ISO/IEC 27001:2013, 7.2), information security risk assessment (ISO/IEC 27001:2013, 8.2), information security risk treatment (ISO/IEC 27001:2013, 8.3); f) includes determining the mechanism for evaluating the effectiveness of the action taken is also planned, and can include monitoring, measurement techniques (ISO/IEC 27001:2013, 9.1), internal audit (ISO/IEC 27001:2013, 9.2) or management review (ISO/IEC 27001:2013, 9.3).
Supporting documents	ISO 31000:2018, 5.3 to 5.7 ISO/IEC 27003:2017, 6.1.1
A.3.1.2 Information security risk assessment (ISO/IEC 27001:2013, 6.1.2)	
Related ISO/IEC 27001 subclauses	ISO/IEC 27001:2013, 8.2
Relevant ISO/IEC 27000 definitions	availability, confidentiality, information security, integrity, risk acceptance, risk analysis, risk assessment, risk criteria, risk identification
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS [ISO/IEC 27001:2013, 6.1.1, 7.5.1 b) and 8.1)]; b) the information security risk assessment process (ISO/IEC 27001:2013, 6.1.2) and the results of information security risk assessment (ISO/IEC 27001:2013, 8.2).
Audit practice guide	Auditors should confirm that an information security risk assessment: a) identifies the security information risks associated with the ISMS; b) consists of risk identification, risk analysis, and risk evaluation processes.
	Risk criteria [ISO/IEC 27001:2013, 6.1.2 a)]
	Auditors should confirm that the organization has established and maintains the risk acceptance criteria and the criteria for performing information security risk assessments. Although the organization is at liberty to consider whatever factors it deems relevant in establishing its risk criteria including risk acceptance criteria and the criteria for performing information security risk assessments, auditors should assess that the organization established its risk criteria including risk acceptance criteria and its criteria for performing information security risk assessments based on informed decision.

Table A.2 *(continued)*

	It is reasonable to expect that the organization's risk criteria are included in the documented information regarding the risk assessment process. If not, the organization should be able to explain to the auditors what they are. At the very least, they should include the organizations' risk acceptance criteria and the criteria for performing risk assessments. NOTE 7 ISO/IEC 27001:2013, 8.2 requires organizations to perform information security risk assessments at planned intervals or when significant changes are proposed or occur. Risk assessment can be performed on all the ISMS or on parts of it (this last case can show when significant changes have impacts on parts of ISMS and then a new partial risk assessment is required).
	Consistency, validity and comparability of results [ISO/IEC 27001:2013, 6.1.2 b)]
	Auditors should confirm that the results of risk assessments by the information security risk assessment process are consistent, valid and comparable. This confirmation can be performed by: — asking the organization why its own risk assessment results are consistent, valid and comparable; — sampling the documented information concerning results of information security risk assessment. For assessing consistency and validity, auditors can verify if: — similar risks in similar contexts have been similarly assessed; — risks differently assessed have a rationale for such difference; — the overall assessment results are unequivocally understandable. For assessing comparability, auditors can verify: — how the same risk has been evaluated in previous risk assessment and if it is understandable if it has changed; — if it is unequivocally understandable if a risk is higher or lower than others.
	Risk identification [ISO/IEC 27001:2013, 6.1.2 c)]
	Auditors should confirm that the organization has identified the information security risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS. NOTE 8 ISO/IEC 27001:2013 does not require the identification of risks by the identification of assets, threats and vulnerabilities. Other methods of risk identification are acceptable, such as identifying risks through a consideration of events and consequences. It is reasonable to expect to find a description of the organization's risk identification process in its documented information concerning the risk assessment process (see below). Factors that the organization can have considered (but need not) in formulating its approach to risk identification can include: a) how risks are found, recognized and described; b) the sources of risk to be considered. Further factors that the organization can have considered (but need not) are: a) how risks can create, enhance, prevent, degrade, accelerate or delay the achievement of the organization's information security objectives; the risks associated with not pursuing an opportunity; b) risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident; c) examination of the knock-on effects of particular consequences, including cascade and cumulative effects; d) consideration of a wide range of consequences, even if the risk source or cause may not be evident;

Table A.2 *(continued)*

	e) consideration of possible causes and scenarios that show what consequences can occur; f) consideration of all significant causes and consequences; g) how a comprehensive list of risks can be generated. NOTE 9 A discovery that large numbers of necessary controls have been inadvertently omitted can be indicative of a weak risk identification process. It should be confirmed on sampling, that all important information within the scope of the ISMS is included in the risk assessment. Auditors should verify that there are risks identified in the documented information regarding the risk assessment results that are associated with the loss of confidentiality, integrity and availability of information within scope of the ISMS. The organization's information security objectives can assist the auditors to identify information security risks. Auditors should also confirm that: a) for each risk, the risk owner(s) have been identified; b) each risk owner has the accountability and authority to manage their identified risk(s).
	Risk analysis [ISO/IEC 27001:2013, 6.1.2 d)]
	Auditors should confirm that: a) the organization comprehends the nature of identified risk and determines the level of the risk, as risk analysis in the information security risk assessment process; b) the risk analysis provides an input to risk evaluation and to decisions on how risks need to be treated and on the most appropriate risk treatment, strategies and methods. Auditors should also confirm that the organization has assessed the potential consequences and likelihoods associated with the risks that it identified in conformance to ISO/IEC 27001:2013, 6.1.2 c) and has thereby determined the levels of risk. It is reasonable to expect to find a description of the organization's approach to risk analysis in the documented information concerning the risk assessment process and the results will be in the documented information regarding the risk assessment results (see below). Auditors should refer to risk management policies, strategies, methods of the organization. Risk analysis can be: a) undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis and the information, data and resources available; b) qualitative, semi-quantitative or quantitative or a combination of these, depending on the circumstances.
	Risk evaluation [ISO/IEC 27001:2013, 6.1.2 e)]
	Auditors should confirm that the organization has compared the results of its risk analysis with the information security risk acceptance criteria to determine the acceptability of the identified risks. Auditors should also confirm that results of the risk assessment(s) reveal as evidence that the risk acceptance criteria have been properly applied and that identified and analysed risks have been prioritized for treatment. In more details, auditors should review that the risk evaluation: a) assists in making decisions, based on the outcomes of risk analysis, about how risks need treatment and the priority for treatment implementation; b) involves comparing the level of risk found during the analysis process with the information security risk criteria established when the context was considered. Auditors should also assess that the decisions: a) take account of the wider context of the risk;

Table A.2 *(continued)*

	b) consider the requirements of relevant interested parties, including legal, regulatory and other requirements.
	Documented information (ISO/IEC 27001:2013, 6.1.2 and 8.2)
	Auditors should confirm that documented information regarding the risk assessment process exists. It would be reasonable to expect that the documented information about the information security risk assessment process will contain: a) a definition of the risk criteria including the risk acceptance criteria and the criteria for performing information security risk assessments; b) rationale for the consistency, validity and comparability of results; c) a description of the risk identification process (including the identification of risk owners); d) a description of the process for analysing the information security risks (including the assessment of potential consequences, realistic likelihood and resultant level of risk); e) a description of the process for comparing the results with the risk criteria and the prioritization of risks for risk treatment. NOTE 10 The above-mentioned items each correspond to an ISO/IEC 27001 requirement, which is why it is reasonable for information about them to be found in the documented information regarding the risk assessment process.
Supporting documents	ISO 31000:2018, 5.3, 5.4, 5.7 ISO/IEC 27003:2017, 6.1.2, 8.2
A.3.1.3 Information security risk treatment (ISO/IEC 27001:2013, 6.1.3)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 8.3, Annex A
Relevant ISO/IEC 27000 definitions	Control, control objective, documented information, information security, residual risk, risk assessment, risk criteria, risk owner, risk treatment
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS; b) the information security risk treatment process; c) the results of information security risk treatment; d) the Statement of Applicability.
Audit practice guide	**Information security risk treatment (ISO/IEC 27001:2013, 6.1.3)**
	Auditors should confirm that the organization modifies information security risks as an information security risk treatment process. Auditors also should review that the information security risk treatment involves: a) selecting one or more options for modifying information security risks, and implementing those options, which provide or modify the controls; b) a cyclical process of assessing the effectiveness of that treatment.
	Select appropriate information security risk treatment options [ISO/IEC 27001:2013, 6.1.3 a)]
	Auditors should confirm that the documented information concerning the risk treatment process contains a description of the method that the organization uses for selecting appropriate information security risk treatment options. Auditors should also confirm that this description corresponds to what the organization actually performs. Note that ISO/IEC 27000:2018, 3.72, Note 1 enumerates seven risk treatment options and there is a note referencing ISO 31000 in ISO/IEC 27001:2013, 6.1.3 from which they are derived.

Table A.2 *(continued)*

	Auditors should verify the consistency between the risk criteria and the risk treatment plan. The organization should be able to explain the decisions that it has made regarding risk treatment options even if they are not documented. Auditors should review the organization's selected risk treatment options. Auditors should also review the appropriateness of the selected risk treatment options. Auditors should verify whether recent changes (e.g. new IT systems or business processes) have been suitably incorporated in the risk assessment and the risk treatment decisions.
	Determine all necessary controls [ISO/IEC 27001:2013, 6.1.3 b)]
	Auditors should confirm that the documented information concerning the risk treatment process contains a description of the method that the organization uses for determining necessary information security controls. Auditors should also confirm that this description corresponds to what the organization actually does. It is a requirement [ISO/IEC 27001:2013, 6.1.3 d)] that the Statement of Applicability contains the necessary controls. The necessary controls do not need to be ISO/IEC 27001:2013, Annex A controls. They may be sector-specific controls (as defined in the sector specific standards, such as ISO/IEC 27011, ISO/IEC 27017). They may also be "custom controls", as organizations can design their own or identified from any source [see ISO/IEC 27001:2013, 6.1.3 b)]. All controls determined to implement the risk treatment options should be included in the Statement of Applicability. Moreover, any custom controls should be explicitly defined as both in requirement and implementation.
	Compare with Annex A [ISO/IEC 27001:2013, 6.1.3 c)]
	Conformance with this requirement is evidenced through review of the Statement of Applicability as described below.
	Produce a Statement of Applicability [ISO/IEC 27001:2013, 6.1.3 d)]
	Auditors should verify that the Statement of Applicability contains: a) the necessary controls as determined by the process of applying ISO/IEC 27001:2013, 6.1.3 b) and c); b) the justification for their inclusion (e.g. by reference to the risk treatment options where it is used); c) whether the necessary controls are implemented or not; d) a justification for all excluded Annex A controls, for example.: 1) the control applies in the context of an activity that the organization does not engage in; 2) the organization uses a custom control that obviates the need for an Annex A control; 3) the organization uses a custom control that serves the same purpose as the Annex A control (see ISO/IEC 27003 for further information); e) relevant sector-specific controls, which will either be designated as necessary controls or treated in the same way as excluded Annex A controls. Auditors should therefore confirm the consistency between the controls necessary to realize selected risk treatment options and the Statement of Applicability.
	Formulate a risk treatment plan [ISO/IEC 27001:2013, 6.1.3 e)]
	Auditors should confirm that the documented information concerning the risk treatment process contains a description of the method that the organization uses for producing its risk treatment plan.
	Auditors should also confirm that the risk treatment plan is formulated from the outputs of ISO/IEC 27001:2013, 6.1.3 a) to c). Auditors should confirm further that the information provided in the treatment plan includes or links to:

Table A.2 *(continued)*

	a) the risk(s) that the plan addresses; b) necessary control(s); c) how the necessary controls are expected to modify the risk so that the risk acceptance criteria are met; d) the risk owners; NOTE 11 The risk owners are responsible for approving the risk treatment plan and accepting the residual risk. e) selected risk treatment option(s); f) the implementation status of necessary controls; g) the reasons for selection of treatment options, including expected benefits to be gained; h) proposed actions including responsible individuals, timeframes and schedule; i) resource requirements including contingencies; j) performance measures and constraints; k) reporting and monitoring. Auditors should review that the risk treatment plan takes into consideration the objective setting and management processes of the organization and is discussed with relevant interested parties.
	Obtain risk owner approval [ISO/IEC 27001:2013, 6.1.3 f)]
	Auditors should confirm that the organization a) identifies appropriate risk owners; b) documents the residual risks; c) obtains the risk owners' approval for the information security risk treatment plan and acceptance of the residual risks.
	Documented information
	Auditors should confirm that documented information regarding the risk treatment process exists. It would be reasonable to expect that the documented information about the information security risk treatment process will contain descriptions of: a) the method for selecting appropriate information security risk treatment options; b) the method for determining necessary controls; c) how ISO/IEC 27001:2013, Annex A is used to determine that necessary controls have not been inadvertently overlooked; d) how the SoA is produced; e) how the risk treatment plan is produced; f) how risk owners' approval is obtained. NOTE 12 There is no particular requirement for the content or format of an organization's risk treatments plan.
Supporting documents	ISO 31000:2018, 5.5, 5.7 ISO/IEC 27003:2017, 6.1.3, 8.3 ISO/IEC 27006
A.3.2 Information security objectives and planning to achieve them (**ISO/IEC 27001:2013**, **6.2**)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 5.1, 5.2, 7.1, 7.3, 7.4, 7.5, 9.1, 9.3, 10.2
Relevant ISO/IEC 27000 definitions	Information security, objective

Table A.2 *(continued)*

Audit evidence	Audit evidence can be obtained through documented information or other information on information security objectives and plans to achieve them.
Audit practice guide	It is noted that there are linkages from information security objectives and planning to achieve them (ISO/IEC 27001:2013, 6.2) to leadership and commitment (ISO/IEC 27001:2013, 5.1) and policy (ISO/IEC 27001:2013, 5.2). Auditors should confirm that: a) information security objectives are established at relevant functions and levels of the organization; b) information security objectives are specified in a way that allows determination of their fulfilment to be made; c) objectives are measurable, if applicable (there can be situations when it may not be feasible to measure an information security objective); d) the status and progress on information security objectives and plans to achieve them are periodically verified in accordance with the requirements of monitoring, measurement, analysis and evaluation (ISO/IEC 27001:2013, 9.1) and updated as appropriate, consistent with the requirements of continual improvement (ISO/IEC 27001:2013, 10.2); e) information security objectives and plans to achieve them are communicated in accordance with the requirements of the communication (ISO/IEC 27001:2013, 7.4); f) documented information of the objectives is created and controlled in accordance with the requirements of documented information (ISO/IEC 27001:2013, 7.5). Auditors should also verify that: a) the actions required to achieve the information security objectives (i.e. "what") and the associated timeframe (i.e. "when") are determined; b) the assignment of responsibility for doing it (i.e. "who") is established in accordance with the requirements of organization roles, responsibilities and authorities (ISO/IEC 27001:2013, 5.3); c) applicable information security requirements, and results from risk assessment and risk treatment are taken into account in the objectives and planning to achieve them; d) any need for budgets, specialized skills, technology or infrastructure, for example, to achieve the objectives are determined and provided in accordance with the requirements of resources (ISO/IEC 27001:2013, 7.1); e) a mechanism for evaluating the overall results of what was accomplished is determined in accordance with the requirements of monitoring, measurement, analysis and evaluation (ISO/IEC 27001:2013, 9.1) and reported in accordance with management review (ISO/IEC 27001:2013, 9.3).
Supporting documents	ISO/IEC 27003:2017, 6.2
A.4 Support (ISO/IEC 27001:2013, Clause 7)	
A.4.1 Resources (ISO/IEC 27001:2013, 7.1)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 5.1, 6.2, 7.2
Relevant ISO/IEC 27000 definitions	Continual improvement, management system
Audit evidence	Audit evidence can be obtained through documented information or other information on the resources that the organization needs to: a) establish and implement the ISMS (including its operations and controls); b) maintain and continually improve the ISMS. Resources can include: a) people;

Table A.2 *(continued)*

	b) specialized skills or knowledge; c) organizational infrastructure (e.g. buildings, communication lines, etc.); d) technology; e) information, other assets associated with information and information processing facilities; f) money (e.g. cash, liquid securities and credit lines).
Audit practice guide	Auditors should confirm that the organization anticipates, determines and allocates the resources needed for establishing and implementing the ISMS (including its operations and controls), as well as those needed for its maintenance and continual improvement.
Supporting documents	ISO 31000:2018, 4.3.5
A.4.2 Competence (ISO/IEC 27001:2011, 7.2)	
Related ISO/ IEC 27001 clauses	ISO/IEC 27001:2013, 5.3, 7.1, 7.5.1 Note, 9.1 d) and e), 9.2 e)
Relevant ISO/IEC 27000 definitions	Competence, effectiveness
Audit evidence	Audit evidence can be obtained through documented information or other information on relevant: a) organizational roles, responsibilities and authorities; b) job descriptions; c) required competence; d) records of education; e) training programmes, courses and educational activities; f) records of actions taken to acquire and retain the necessary competence; g) evaluation of their effectiveness. ISO/IEC 27001:2013, 7.2 broadens the scope of competence to persons who are not members of the organization. The requirement specifies that they are "doing work under the control of the organization". Examples can include subcontractors and volunteer workers. Audit evidence requested from a third party should be restricted to evidence of the functions and activities performed for the ISMS organization
Audit practice guide	Auditors should confirm that the organization: a) determines: 1) the persons doing work under its control that affects its information security performance; 2) the knowledge and skills for the persons to achieve intended results; 3) the ability of the persons to apply the knowledge and skills to achieve intended results; b) ensures that these persons have the ability on the basis of appropriate education, training, or experience; c) where applicable, takes actions to acquire the necessary ability and evaluate the effectiveness of the actions taken.
Supporting documents	ISO/IEC 27003:2017, 7.2 ISO/IEC 27021:2017, Annex A
A.4.3 Awareness (ISO/IEC 27001:2013, 7.3)	

Table A.2 *(continued)*

Related ISO/ IEC 27001 clauses	ISO/IEC 27001:2013, 5.1 d), 5.2, 9.1, 9.2, 10.1, 10.2
Relevant ISO/IEC 27000 definitions	Conformity, effectiveness, performance, policy
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) information security policy; b) information security objectives; c) information security performance; d) nonconformity and corrective action; e) organizational roles, responsibilities and authorities; f) job descriptions; g) awareness programmes and training material, where applicable.
Audit practice guide	Auditors should confirm that persons doing work under the organization's control are aware of: a) the information security policy; b) their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance; c) the implications of not conforming with the ISMS requirements. Auditors should interview an appropriate number of persons as sampling to confirm that they are aware of this information. Awareness of the policy should not be taken to mean that it needs to be memorized; rather, persons should be aware of the key policy commitments, and their role in achieving them. Auditors can find information security awareness evidence also in awareness and training initiatives not dedicated to information security. These activities can be closely related to the communication activities by top management [ISO/IEC 27001:2013, 5.1 d) and 7.4].
Supporting documents	ISO/IEC 27003:2017, 7.3
A.4.4 Communication (ISO/IEC 27001:2013, 7.4)	
Related ISO/ IEC 27001 clauses	ISO/IEC 27001:2013, 5.1, 5.2, 5.3, 6.2, 9.2
Relevant ISO/IEC 27000 definitions	Policy
Audit evidence	Audit evidence can be obtained through documented information or other information on a) information security policy; b) organizational roles, responsibilities and authorities; c) the information security risk assessment process; d) the information security risk treatment process; e) information security objectives; f) information that the processes have been carried out as planned; g) the results of the information security risk assessments; h) the results of the information security risk treatment; i) performance of the ISMS; j) results of audits;

Table A.2 *(continued)*

	k) results of management reviews.
Audit practice guide	Auditors should confirm that the organization's communication needs are identified, implemented and maintained effectively along the communication requirements of ISO/IEC 27001. Examples of evidence can include a) answers being documented in the minutes of a meeting, or b) a formal communications plan, documented procedures and results, or c) interviews with people assigned to defined roles in order to demonstrate that they know, for communication relevant to their roles, on what, when, whom to communicate, who have authorities for such communication and how it is the processes by which communication is affected. Such evidence can be supplemented by: a) information of communication on the following: 1) importance of effective information security management and of conforming to the information security management system requirements; 2) policy; 3) responsibilities and authorities; 4) performance of the ISMS; 5) objectives; 6) contribution to the effectiveness of the ISMS, including the benefits of improved performance; 7) implications of not conforming with the ISMS requirements; 8) results of audits; b) a formal communications plan, documented procedures and results. Auditors should verify that the organization has determined its needs for communication related to the ISMS. For example, these can include transparency, appropriateness, credibility, responsiveness, clarity and protection. Communication can be verbal or written, one-way or two-way, internal or external.
Supporting documents	ISO 31000:2018, 4.3.6, 4.3.7 ISO/IEC 27003:2017, 7.4
A.4.5 Documented information (ISO/IEC 27001:2013, 7.5)	
A.4.5.1 General (ISO/IEC 27001:2013, 7.5.1)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, and 10.1
Relevant ISO/IEC 27000 definitions	Documented information
Audit evidence	Audit evidence can be obtained through documented information or other information created, controlled and/or maintained in an ISMS, including: a) scope of the management system; b) policy; c) objectives; d) evidence of competence; e) information of external origin necessary for the planning and operation of the management system;

Table A.2 *(continued)*

	f) information security risk assessment process; g) information security risk treatment process; h) Statement of Applicability; i) information necessary to have confidence that the processes and determined controls have been carried out as planned; j) results of information security risk assessment; k) results of information security risk treatment; l) monitoring, measurement, analysis and evaluation results; m) internal audit programme and evidence of its implementation; n) internal audit results; o) management review results; p) nature of nonconformities and actions taken; q) corrective action results. Documented information, originally created for purposes other than the fulfilment of the requirements of ISO/IEC 27001, can be used.
Audit practice guide	Auditors should confirm that the organization's ISMS includes: a) documented information required by ISO/IEC 27001; b) documented information determined by the organization as being necessary for the effectiveness of the ISMS. The phrase "documented information as evidence of ..." implies the former term "record". Auditors should confirm that the organization determines what documented information it needs beyond that which is explicitly required by ISO/IEC 27001 for the effectiveness of its ISMS. The factors it should take into account are listed in the row of audit evidence. The term "documented information" refers to information that ISO/IEC 27001 determines is necessary to control and maintain in any format or media (see ISO/IEC 27001:2013, 7.5.3). The auditor should confirm that documented information is created and controlled in accordance with the requirements of ISO/IEC 27001:2013, 7.5.2 and 7.5.3.
Supporting documents	ISO 31000:2018, 5.7 ISO/IEC 27003:2017, 7.5.1
A.4.5.2 Creating and updating (ISO/IEC 27001:2013, 7.5.2)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, and 10.1
Relevant ISO/IEC 27000 definitions	Documented information
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) common attributes which allow clear and unique identification; b) format and media used; c) date of last review or update; d) history of changes; e) identity of reviewer and approver.
Audit practice guide	Auditors should confirm that when creating and updating documented information, the organization ensures appropriate a) identification and description (e.g. a title, date, author, or reference number); b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); c) review and approval for suitability and adequacy documented information.

Table A.2 *(continued)*

	NOTE 13 The identification, format and media used for documented information are the choice of the organization implementing ISO/IEC 27001; it need not be in the form of a textual format or a paper manual. Auditors should take the opportunity to carry out these audit tasks whenever documented information within scope of the ISMS is presented to the audit. They do not need to be performed each and every time, just a sufficient number to confirm conformity to ISO/IEC 27001:2013, 7.5.2.
Supporting documents	ISO/IEC 27003:2017, 7.5.2
A.4.5.3 Control of documented information (ISO/IEC 27001:2013, 7.5.3)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, and 10.1
Relevant ISO/IEC 27000 definitions	Documented information
Audit evidence	Audit evidence can be obtained through documented information or other information on the following activities: a) distribution, access, retrieval and use; b) storage and preservation, including the preservation of legibility; c) control of changes (e.g. version control); d) retention and disposition; e) structure and configuration of documented information library.
Audit practice guide	Auditors should confirm that documented information required by the ISMS and by ISO/IEC 27001 is controlled to ensure that: a) it is available and suitable for use, where and when it is needed; b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). The auditor should confirm that the organization addresses the following activities, as applicable: a) distribution, access, retrieval and use; b) storage and preservation, including the preservation of legibility (in digital or other formats or hand-written); c) control of changes (e.g. version control); d) retention and disposition. Auditors should take the opportunity to carry out these audit tasks whenever documented information within the scope of the ISMS is presented to the audit. They do not have to be performed each and every time, just a sufficient number to confirm conformity to ISO/IEC 27001:2013, 7.5.3.
Supporting documents	ISO 31000:2018, 5.7 ISO/IEC 27003:2017, 7.5.3
A.5 Operation (ISO/IEC 27001:2013, Clause 8)	
A.5.1 Operational planning and control (ISO/IEC 27001:2013, 8.1)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 4.4, 6.1.1, 6.1.2, 6.1.3, 6.2, 7.5.1, 9.1, and 9.2
Relevant ISO/IEC 27000 definitions	Consequence, information security, objective, organization, outsource, process, requirement

Table A.2 *(continued)*

Audit evidence	Audit evidence can be obtained through documented information or other information which is: a) needed for the organization to have confidence that the operational control processes have been carried out as planned is created and controlled (ISO/IEC 27001:2013, 8.1); b) determined by the organization as being necessary for the effectiveness of the ISMS [ISO/IEC 27001:2013, 7.5.1 b)]; c) on planning for the ISMS (ISO/IEC 27001:2013, 6.1.1); d) on information security objectives (ISO/IEC 27001:2013, 6.2).
Audit practice guide	Auditors should confirm that the organization plans, implements and controls the processes needed to meet information security requirements within the organization's operations to make sure that the requirements of ISO/IEC 27001 are fulfilled and the priority risks and opportunities are being addressed. Auditors should confirm that the operational control includes the methods and information security controls implemented to make sure business operations, activities or equipment conform to specified conditions, performance standards or regulatory compliance limits, and thereby effectively achieve the intended outcome of the ISMS. These controls establish technical requirements necessary to achieve the desired optimal functionality for business processes, such as technical specifications or operating parameters or a prescribed methodology. Reviewing should be performed for the situations which the operational control and information security controls are required for, related to business processes where absence of the operational control and information security controls could lead to deviations from the policy and objectives or poses unacceptable risk. These situations can be related to business operations, activities or processes, production, installation or servicing, maintenance or contractors, suppliers or vendors. The degree of control exercised will vary depending on many factors, including the functions performed, their importance or complexity, the potential consequences of deviation or variability or the technical competency involved versus what is available. Auditors should thereby verify that the organization: a) implements the actions determined in "actions to address risks and opportunities" (ISO/IEC 27001:2013, 6.1); b) implements the plans to achieve information security objectives determined in Information security objectives and planning to achieve them (ISO/IEC 27001:2013, 6.2); c) creates and controls documentation needed to have confidence that the operational control processes and information security controls have been carried out as planned in accordance with the requirements of documented information (ISO/IEC 27001:2013, 7.5); d) controls planned changes and reviews the consequences of unintended changes, to prevent or otherwise minimize the chance technical requirements are not fulfilled or new risks are introduced; e) takes actions necessary to address any resultant undesired effect(s) when operational controls fail; f) ensures that outsourced processes are determined and controlled, i.e. applies the control of operations under considerations such that the degree of control can be limited to partial control or influence and be not intended to change any legal relationship with the external entity performing the outsourced process.
Supporting documents	ISO/IEC 27003:2017, 8.1
A.5.2 Information security risk assessment (ISO/IEC 27001:2013, 8.2)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 6.1.2

Table A.2 *(continued)*

Relevant ISO/IEC 27000 definitions	Information security
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS (ISO/IEC 27001:2013, 6.1.1); b) the information security risk assessment process (ISO/IEC 27001:2013, 6.1.2); c) the results of information security risk assessment (ISO/IEC 27001:2013, 8.2); d) the Statement of Applicability; e) the risk treatment plans.
Audit practice guide	Auditors should confirm that the information security risk assessment process defined and applied in (ISO/IEC 27001:2013, 6.1) is implemented and integrated into the organizational operations and be performed at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in ISO/IEC 27001:2013, 6.1.2 a). Auditors should assess that: a) the planned intervals at which the risk assessment is performed are appropriate to the ISMS; b) when any significant changes of the ISMS (or its context) or information security incidents have occurred, the organization determines which of these changes or incidents require an additional information security risk assessment and how these assessments are triggered. For additional information, see audit practice guide of A.3.1.2.
Supporting documents	ISO 31000:2018, 5.4.1 ISO/IEC 27003:2017, 8.2 ISO/IEC 27005
A.5.3 Information security risk treatment (ISO/IEC 27001:2013, 8.3)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 6.1.3, Annex A
Relevant ISO/IEC 27000 definitions	Control, control objective, documented information, information security, residual risk, risk assessment, risk criteria, risk owner, risk treatment
Audit evidence	Audit evidence can be obtained through documented information or other information on: a) planning for the ISMS; b) the information security risk treatment process; c) the risk treatment plans; d) the results of information security risk treatment; e) the Statement of Applicability.
Audit practice guide	Auditors should confirm that the information security risk treatment process defined and applied in "Planning the ISMS" (ISO/IEC 27001:2013, 6.1) is implemented and integrated into the organizational operations, and be performed after each iteration of the information security risk assessment process (ISO/IEC 27001:2013, 8.2) or when the implementation of (parts of) the risk treatment has failed. For additional information, see audit practice guide of A.3.1.3.
Supporting documents	ISO 31000:2018, 5.5 ISO/IEC 27003:2017, 8.3 ISO/IEC 27005
A.6 Performance evaluation (ISO/IEC 27001:2013, Clause 9)	
A.6.1 Monitoring, measurement, analysis and evaluation (ISO/IEC 27001:2013, 9.1)	

Table A.2 *(continued)*

Related ISO/ IEC 27001 clauses	ISO/IEC 27001:2013, 5.3 b), 6.1.1 e), 6.2
Relevant ISO/IEC 27000 definitions	Continual improvement, effectiveness, measurement, monitoring, performance, information security event, information security incident, information need, measure
Audit evidence	Audit evidence can be obtained through documented information or other information on the results of monitoring, measurement, analysis and evaluation (see ISO/ IEC 27001:2013, 9.1). Evidence can also be obtained through documented information or other information about: a) information security objectives at relevant functions and levels; b) planning how to achieve the information security objectives; c) the status of and extent to which the information security objectives are fulfilled; d) reporting on the performance of the ISMS to top management [see ISO/IEC 27001:2013, 5.3 b)]; e) results of risk assessment and status of risk treatment plan; f) the methods for monitoring, measurement, analysis and evaluation; g) internal audit programme(s) and the audit results; h) management review(s) and the management reviews' results; i) information security events reports (see ISO/IEC 27001:2013, A.16.1.2); j) information security weaknesses reports (see ISO/IEC 27001:2013, A.16.1.3); k) information security incidents reports (see ISO/IEC 27001:2013, A.16.1.4).
Audit practice guide	Auditors should confirm that the organization has: a) evaluated the information security performance and effectiveness of its ISMS; b) has thereby determined: 1) what to be monitored and measured (qualitatively and quantitatively), including information security processes and controls; 2) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; 3) when the monitoring and measuring is to be performed; 4) who performs monitoring and measurement; 5) when the results from monitoring and measurement are to be analysed and evaluated; 6) who conducts analysis and evaluation of these results. Auditors should review the information security performance using documented information as evidence such as plans, reports on the performance of the ISMS to top management, the results of management review, internal audit reports and information security event, weakness incident reports. Auditors should assess the extent to which nonconformities, processing errors, information security breaches and other incidents are predicted, detected, reported and addressed. Auditors should determine whether and how the organization evaluates the effectiveness of the actions to address the risks and opportunities to ensure that the information security controls identified in the risk treatment, are effectively implemented and be in operation.

Table A.2 *(continued)*

	Auditors should also assess the evaluation of information security performance for being used to drive continual improvements of the ISMS. Auditors should also confirm that changes to be considered (ISO/IEC 27001:2013, 8.1 and 8.2) as of the results are reflected in the processes for risk assessment and risk treatment processes. In addition, auditors should confirm that the documented information related to the actions to address risk and opportunities have been updated. Auditors should review that the information of characteristics that are monitored or measured, analysed and evaluated is necessary and sufficient enough to judge the extent to which the ISMS planned activities are realized and its planned results are achieved. Auditors should confirm that the information gained through monitoring or measurement, analysis and evaluation is presented to top management in accordance with the requirements of management review (ISO/IEC 27001:2013, 9.3). NOTE 14 If an organization follows the guidance given in ISO/IEC 27004, in addition to "information need", it can use the terms "performance measure" and "effectiveness measure".
Supporting documents	ISO/IEC 27004
A.6.2 Internal audit (ISO/IEC 27001:2013, 9.2)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 9.3
Relevant ISO/IEC 27000 definitions	Audit, audit scope, competence
Audit evidence	Audit evidence can be obtained through documented information or other information about: a) an internal audit programme(s); b) internal audit plans; c) internal audit results; d) competence of internal auditors; e) results of management reviews.
Audit practice guide	NOTE 15 This subclause provides guidance to external auditing or self-checking or peer assessment guidance regarding internal auditing. Auditors should confirm that the organization plans, implements and maintains an internal audit programme for the purpose of providing information on whether the ISMS conforms to both ISO/IEC 27001 requirements and any additional ISMS related requirements the organization self imposes and that the ISMS is being effectively implemented and maintained as planned. Auditors should verify that the internal audit programme is such that: a) internal audits are planned and scheduled based on the importance of the processes audited and the results of previous audits; b) the approach for planning and conducting internal audits is established; c) roles and responsibilities within the audit programme are assigned by taking into account the integrity and independence of the internal audit process; d) the audit objectives, audit criteria and audit scope are established for each audit planned; e) it is designed to provide information to confirm that the ISMS conforms to: 1) the requirements of ISO/IEC 27001; 2) the organization's own requirements; f) it is designed to provide information to confirm that the ISMS is effectively implemented and maintained.

Table A.2 *(continued)*

	An example of an audit criterion is a reference (e.g. policies, procedures and requirements) against which relevant and verifiable records, statements of fact or other information will be compared. Audit scopes can include descriptions of the physical locations, organizational units, activities and processes, as well as the time period covered for the audits concerned. Auditors should confirm that the internal audit programme and the audits are planned and implemented and maintained by internal personnel, or be managed by external persons acting on the organization's behalf. In either case, auditors should confirm that the selection of persons responsible for managing the internal audit programme and the auditors who conduct the internal audits meet competence (see ISO/IEC 27001:2013, 7.2 and 9.2) requirements and guidelines (see ISO/IEC 27001:2013, 7.2). Auditors should confirm that the results of internal audits are reported to the management responsible for the functions/unit audited and any other individuals deemed appropriate in accordance with the requirements of communication (ISO/IEC 27001:2013, 7.4). Auditors should confirm that the information, including trends, on internal audit results is reviewed in accordance with the requirements of management review (see ISO/IEC 27001:2013, 9.3).
Supporting documents	This document, i.e. ISO/IEC 27007 ISO/IEC TS 27008 ISO/IEC 17021-1:2015, 9.3.1.2.2 g), 9.3.1.3 e), 9.4.8.3 a), 9.6.2.2 a) ISO/IEC 27006:2015, 9.1.5.1, 9.3.1.2.2 h), 9.5.1, 9.6.2.1.1 a)
A.6.3 Management review (ISO/IEC 27001:2013, 9.3)	
Related ISO/IEC 27001 clauses	ISO/IEC 27001:2013, 4.1, 4.2, 8.1.2, 8.1.3, 9.1, 9.2, 10.1, and 10.2
Relevant ISO/IEC 27000 definitions	Continual improvement, effectiveness, performance
Audit evidence	Audit evidence can be obtained through documented information or other information about: a) conducting the reviews at planned intervals; b) the status of actions from previous management reviews; c) changes in external and internal issues that are relevant to the ISMS; d) feedback on the information security performance, including trends in nonconformities and corrective actions, monitoring and measurement results, audit results and fulfilment of information security objectives; e) feedback from interested parties; f) results of risk assessment and status of risk treatment plan; g) opportunities for continual improvement.
Audit practice guide	Auditors should confirm that top management has conducted management reviews in accordance with a planned schedule of reviews, reviewing the information to be covered and providing the expected outputs. Auditors should assess through auditing that the top management be personally engaged in this review, carrying out this mechanism to drive changes to the ISMS and direct continual improvement priorities, particularly in relation to the changing issues in the organization's context, deviations from intended results or favourable conditions that offer an advantage with beneficial outcome. Auditors should verify that the management review includes consideration of all the items b) to g) listed in the audit evidence of A.6.3. Auditors should also confirm that the outputs of the management review include decisions related to continual improvement opportunities and any needs for changes to the ISMS.
A.7 Improvement (ISO/IEC 27001:2013, Clause 10)	
A.7.1 Nonconformity and corrective action (ISO/IEC 27001:2013, 10.1)	

Table A.2 *(continued)*

Related ISO/ IEC 27001 clauses	ISO/IEC 27001:2013, 7.5, 8.1, 10.2
Relevant ISO/IEC 27000 definitions	Correction, corrective action, effectiveness, nonconformity
Audit evidence	Audit evidence can be obtained through documented information or other information about: a) the nature of the nonconformities and any subsequent actions taken; b) the results of any corrective action; c) monitoring and measurement results; d) audit programme(s) and the audit results; e) the results of management review; f) the requirements of interested parties relevant to information security; g) the changes to the ISMS brought by corrective actions.
Audit practice guide	Auditors should confirm that: a) the organization responds by finding nonconformity and requiring corrective action when ISO/IEC 27001 and ISMS (including operational) requirements are not satisfied; b) the nonconformity and corrective action includes taking action to correct the situation, examine the cause and determine if other occurrences exist or potentially exist elsewhere so that action can be taken to prevent recurrence; c) the organization's response covers evaluation of the action taken to confirm that the intended result was achieved, and evaluation of the ISMS to determine if changes are warranted to avoid future occurrences of similar nonconformities; d) documentation of the nonconformity, corrective action and the results is created and controlled in accordance with the requirements of documented information (see ISO/IEC 27001:2013, 7.5).
Supporting documents	
A.7.2 Continual improvement (ISO/IEC 27001:2013, 10.2)	
Related ISO/ IEC 27001 clauses	ISO/IEC 27001:2013, 5.1, 5.2, 6.1, 6.2, 7.1, 8.1, 9.1, 9.2, 9.3, 10.1
Relevant ISO/IEC 27000 definitions	Continual improvement, effectiveness, performance
Audit evidence	Audit evidence can be obtained through documented information or other information about: a) the nature of nonconformities and any subsequent actions taken, including reporting of corrective actions; b) the results of any corrective action; c) monitoring and measurement results; d) audit programme(s) and the audit results; e) the results of management review; f) the requirements of interested parties relevant to information security; g) assessment of and decision on information security events and incidents (see ISO/IEC 27001:2013, A.16.1.4).
Audit practice guide	Auditors should confirm that the organization conducts its recurring activity to enhance measurable results of the suitability, adequacy and effectiveness of the ISMS.

Table A.2 *(continued)*

	Auditors should review and verify that the continual improvement involves making changes to the design and implementation of the ISMS in order to improve the organization's ability to achieve conformity with the requirements of the ISMS and meet its objectives and policy commitments. Auditors should confirm through auditing that the organization: a) develops a implementation to achieve this improvement, including, but not limited to: 1) taking actions to address risks and opportunities (see ISO/IEC 27001:2013, 6.1); 2) establishing objectives (see ISO/IEC 27001:2013, 6.2); 3) upgrading operational controls (see ISO/IEC 27001:2013, 8.1), taking into consideration new technologies, methods or information; 4) analysing and evaluating performance (see ISO/IEC 27001:2013, 9.1); b) conducts internal audits (see ISO/IEC 27001:2013, 9.2); c) conducts management reviews (see ISO/IEC 27001:2013, 9.3); d) detects non-conformity(ies) and implements corrective action(s) (see ISO/IEC 27001:2013, 10.1); e) periodically evaluates and reviews its ISMS in accordance with the requirements of monitoring, measurement, analysis and evaluation (ISO/IEC 27001:2013, 9.1) and internal audit (ISO/IEC 27001:2013, 9.2) and management review (ISO/IEC 27001:2013, 9.3) to identify opportunities for improvement and plans appropriate actions to be taken in accordance with actions to address risks and opportunities (ISO/IEC 27001:2013, 6.1), objectives and planning to achieve them (ISO/IEC 27001:2013, 6.2) and operational planning and controls (ISO/IEC 27001:2013, 8.1).

Bibliography

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

[2] ISO/IEC 17024, *Conformity assessment — General requirements for bodies operating certification of persons*

[3] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[4] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[5] ISO/IEC 27003:2017, *Information technology — Security techniques — Information security management systems — Guidance*

[6] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[7] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[8] ISO/IEC 27006:2015, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[9] ISO/IEC TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[10] ISO/IEC 27021:2017, *Information technology — Security techniques — Competence requirements for information security management systems professionals*

[11] ISO 31000:2018, *Risk management — Guidelines*

[12] IAF MD1, 2018, IAF Mandatory Document for the Audit and Certification of a Management system Operated by Multi-Site Organization, International Accreditation Forum. [viewed 2019-01-01]. Available at https://www.iaf.nu/articles/Mandatory_Documents_/38

ICS 35.030; 03.120.20

Price based on 39 pages