INTERNATIONAL STANDARD

ISO/IEC 27007

First edition
2011-11-15

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

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27007:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

Introduction

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

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

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

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

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

1 Scope

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

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 19011:2011, *Guidelines for auditing management systems*

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

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

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

4 Principles of auditing

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

5 Managing an audit programme

5.1 General

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

5.1.1 IS 5.1 General

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

5.2 Establishing the audit programme objectives

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

5.2.1 IS 5.2 Establishing the audit programme objectives

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

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

Examples of audit programme objectives may include the following:

1) verification of conformity with the identified legal and contractual requirements and other requirements and their security implications;

2) Obtaining and maintaining confidence in the risk management capability of an auditee.

5.3 Establishing the audit programme

5.3.1 Role and responsibilities of the person managing the audit programme

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

5.3.2 Competence of the person managing the audit programme

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

5.3.3 Determining the extent of the audit programme

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

5.3.3.1 IS 5.3.3 Determining the extent of the audit programme

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

a) the size of the ISMS, including
    1. the total number of personnel working at each location and relationships with third-party contractors working regularly at the location to be audited;
    2. the number of information systems;
    3. the number of sites covered by the ISMS;
b) the complexity of the ISMS (including the number and criticality of processes and activities);
c) the significance of the information security risks identified for the ISMS;
d) the importance of information and related assets within the scope of the ISMS;

---

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

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

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

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

5.3.4 Identifying and evaluating audit programme risks

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

5.3.5 Establishing procedures for the audit programme

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

5.3.6 Identifying audit programme resources

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

5.3.6.1 IS 5.3.6 Identifying audit programme resources

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

5.4 Implementing the audit programme

5.4.1 General

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

5.4.1.1 IS 5.4.1 General

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

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

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

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

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

The audit objectives may in addition include the following:

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

Practical help — Examples of audit criteria

The following are topics for consideration as audit criteria:

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

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

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

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

5.4.3 Selecting the audit methods

The guidelines from ISO 19011:2011, Clause 5.4.3, apply. In addition, the following ISMS-specific guidance applies.

5.4.3.1 IS 5.4.3 Selecting the audit methods

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

5.4.4 Selecting the audit team members

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

5.4.4.1 IS 5.4.4 Selecting the audit team members

The competence of the overall audit team should include:

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

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

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

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

5.4.6 Managing the audit programme outcome

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

5.4.7 Managing and maintaining audit programme records

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

5.5 Monitoring the audit programme

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

5.6 Reviewing and improving the audit programme

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

6 Performing an audit

6.1 General

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

6.2 Initiating the audit

6.2.1 General

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

6.2.2 Establishing initial contact with the auditee

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

6.2.3 Determining the feasibility of the audit

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

6.2.3.1 IS 6.2.3 Determining the feasibility of the audit

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

6.3 Preparing audit activities

6.3.1 Performing document review in preparation for the audit

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

6.3.2 Preparing the audit plan

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

6.3.3 Assigning work to the audit team

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

6.3.4 Preparing work documents

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

6.4 Conducting the audit activities

6.4.1 General

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

6.4.2 Conducting the opening meeting

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

6.4.3 Performing document review while conducting the audit

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

6.4.3.1 IS 6.4.3 Performing document review while conducting the audit

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

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

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

6.4.4 Communicating during the audit

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

6.4.5 Assigning roles and responsibilities of guides and observers

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

6.4.6 Collecting and verifying information

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

6.4.6.1 IS 6.4.6 Collecting and verifying information

Gathering information and evidence that ISMS processes and controls are implemented and effective is an important part of ISMS auditing. Possible methods to collect relevant information during the audit include:

a) review of information assets and the ISMS processes and controls implemented for them; and
b) use of automated audit tools.

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

ISMS auditors should ensure appropriate handling of all information received from auditees according to the agreement between the auditee and the audit team.

6.4.7 Generating audit findings

The guidelines from ISO 19011:2011, Clause 6.4.7, apply.

6.4.8 Preparing audit conclusions

The guidelines from ISO 19011:2011, Clause 6.4.8, apply.

6.4.9 Conducting the closing meeting

The guidelines from ISO 19011:2011, Clause 6.4.9, apply.

6.5 Preparing and distributing the audit report

6.5.1 Preparing the audit report

The guidelines from ISO 19011:2011, Clause 6.5.1, apply.

6.5.2 Distributing the audit report

The guidelines from ISO 19011:2011, Clause 6.5.2, apply.

6.6 Completing the audit

The guidelines from ISO 19011:2011, Clause 6.6 apply.

6.7 Conducting audit follow-up

The guidelines from ISO 19011:2011, Clause 6.7 apply.

7 Competence and evaluation of auditors

7.1 General

The guidelines from ISO 19011:2011, Clause 7.1 apply.

7.2 Determining auditor competence to fulfil the needs of the audit programme

7.2.1 General

The guidelines from ISO 19011:2011, Clause 7.2.1 apply. In addition, the following ISMS-specific guidance applies.

7.2.1.1 IS 7.2.1 General

In deciding the appropriate knowledge and skills, the following should be considered:

a) complexity of the ISMS (e.g. criticality of information systems, risk situation of the ISMS) ;
b) the type(s) of business performed within the scope of the ISMS;
c) extent and diversity of technology utilized in the implementation of the various components of the ISMS (such as the implemented controls, documentation and/or process control, corrective/preventive action, etc.);
d) number of sites;
e) previously demonstrated performance of the ISMS;
f) extent of outsourcing and third party arrangements used within the scope of the ISMS;
g) the standards, legal requirements and other requirements relevant to the audit programme.

7.2.2 Personal behaviour

The guidelines from ISO 19011:2011, Clause 7.2.2 apply.

7.2.3 Knowledge and skills

7.2.3.1 General

The guidelines from ISO 19011:2011, Clause 7.2.3.1, apply.

7.2.3.2 Generic knowledge and skills of management system auditors

The guidelines from ISO 19011:2011, Clause 7.2.3.2, apply.

7.2.3.3 Discipline and sector specific knowledge and skills of management system auditors

The guidelines from ISO 19011:2011, Clause 7.2.3.3, apply. In addition, the following ISMS-specific guidance applies.

7.2.3.3.1 IS 7.2.3.3 Discipline and sector specific knowledge and skills of management system auditors

ISMS auditors should have knowledge and skills in the following areas:

a) Information security management methods: to enable the auditor to examine ISMS and generate the appropriate audit findings and recommendations. Knowledge and skills in this area should include:
    1) information security terminology;
    2) information security management principles and their application; and
    3) information security risk management methods and their application.
b) General knowledge in information technology and information security techniques, as applicable (for example, physical and logical access control techniques; protection against malicious software; vulnerability management techniques, etc.), or access thereto.
c) Current information security threats, vulnerabilities and controls, plus the broader organizational, legal and contractual context for the ISMS (e.g. changing business processes and relationships, technology or laws).

If additional specific knowledge and/or skills are required, the use of information security experts (e.g. with sector specific competence, competence in IT Security or business continuity management) should be considered. If experts are used, their competence should be carefully evaluated.

NOTE Specific requirements for ISMS certification auditors are given in ISO/IEC 27006.

7.2.3.4 Generic knowledge and skills of an audit team leader

The guidelines from ISO 19011:2011, Clause 7.2.3.4, apply.

7.2.3.5 Knowledge and skills for auditing management systems addressing multiple disciplines

The guidelines from ISO 19011:2011, Clause 7.2.3.5, apply.

7.2.4 Achieving auditor competence

The guidelines from ISO 19011:2011, Clause 7.2.4, apply. In addition, the following ISMS-specific guidance applies.

7.2.4.1 IS 7.2.4 Achieving auditor competence

ISMS auditors should have knowledge and skills in information technology and information security, demonstrated for example through relevant certifications, and should also be able to understand the respective business requirements. ISMS auditors' work experience should also contribute to the development of their knowledge and skills in the ISMS field.

7.2.5 Audit team leader

The guidelines from ISO 19011:2011, Clause 7.2.5, apply.

7.3 Establishing the auditor evaluation criteria

The guidelines from ISO 19011:2011, Clause 7.3, apply.

7.4 Selecting the appropriate auditor evaluation method

The guidelines from ISO 19011:2011, Clause 7.4, apply.

7.5 Conducting auditor evaluation

The guidelines from ISO 19011:2011, Clause 7.5, apply.

7.6 Maintaining and improving auditor competence

The guidelines from ISO 19011:2011, Clause 7.6, apply.

Annex A
(informative)

Practice Guidance for ISMS Auditing

The text below provides generic guidance on how to audit the ISMS processes, as required by ISO/IEC 27001, without regard to any specific ISMS requirements that an individual organization might have (for example, legal and contractual requirements and other requirements relevant to the implementation of particular information security controls).

This guidance is primarily intended to be referenced and used by auditors who will perform ISMS auditing, be they internal or external.

Optional additional standards can be used to guide the auditee or auditor. These are listed as "Relevant Standards" in the tables below. Auditors are reminded to base nonconformities solely on the audit criteria and the requirements of ISO/IEC 27001.

Table A.1 — ISMS audit practice guidance

A.1 ISMS scope, policy and risk assessment approach (ISO/IEC 27001 4.1 & 4.2.1a) to c))	
Audit criteria	ISO/IEC 27001[2)] 4.1, 4.2.1 a), b) and c)
Relevant standards	ISO/IEC 17021 9.2.1 a) to d) ISO/IEC 27005 3.1 to 3.9 (ISO/IEC Guide73) ISO/IEC 27005 7.1,7.2, 7.3 and 7.4 ISO/IEC 27006 3.1, 3.5, 9.1.2 and 9.1.4.2 b) to d)
Audit evidence	Audit evidence includes: • Scope of the ISMS (4.3.1 b)); • Organization chart; • Organization strategy; • Business policy statement, business processes and activities; • Documentation of roles and responsibilities; • Network configuration; • Sites information, including a list of branches, business, offices and facilities, and their floor layouts; • Interfaces and dependencies that the business activities carried out in the scope of the ISMS have with those outside the scope; • Relevant laws, regulations and contracts; • Primary assets information; • ISMS policy document.
Audit practice guide	**Information security management system (4)**
	General requirements (4.1)
	"4.1 General requirements" in ISO/IEC 27001 specifies the overall context of an ISMS as required by ISO/IEC 27001, which covers all the requirements stated in the clauses subsequent to 4.1. In auditing practice, an ISMS has to be confirmed as being: • organized and performed within the context of the organization's overall business activities and the risks it faces;

2) Undated references refer to the version of the standard cited in Normative References or Bibliography.

- documented to satisfy the documentation requirements (stated in 4.3).

In addition, it should be demonstrated that the ISMS has been established, implemented, operated, monitored, reviewed, maintained and improved, e.g. the organization demonstrates that it has the capability of carrying out these processes.

Establishing and managing the ISMS (4.2)

Establish the ISMS (4.2.1)

ISMS scope (4.2.1 a))

The auditor should review and confirm that the organization has defined the scope and boundaries of the ISMS.

The scope of the ISMS needs to be identified to ensure that all relevant assets are taken into account in the ISMS and its risk management. In addition, the boundaries, interfaces and dependencies need to be identified to address those risks that might arise through them.

It should be confirmed that information about the organization has been collected to determine the context within which the organization operates and how the organization has been related to the ISMS and its information security risk management processes, in order to define the scope and boundaries.

The auditor should confirm that the organization has considered the following information in order to define the scope and boundaries:

- organization's strategies, business objectives and policies;
- business processes;
- organization's functions and structure;
- legal and contractual requirements and other requirements relevant to the organization;
- primary information assets;
- locations of the organization and their geographical characteristics;
- constraints affecting the organization;
- expectation of stakeholders;
- socio-cultural environment; and
- interfaces (i.e. information exchange with the environment).

It should be reviewed and verified that the organization provides justification for any exclusion from the scope. It should be confirmed that the organization has its own functions and administration and is able to ensure that the ISMS is exercised continually all through its life cycle (ISO/IEC 27001 Section 4.1 and ISO/IEC 27006 Section 3.5).

Further guidance on how to audit the ISMS scope is given in Section 6.2.3.

ISMS policy (4.2.1 b))

The auditor should confirm that the organization's ISMS policy is specifically described in terms of the characteristics of the business, the organization, its location, assets and technology. The auditor should also confirm that the ISMS policy clearly identifies:

- a framework for setting ISMS objectives (the background to and rationale for setting the objectives, and if the ISMS policy and information security policies are described in one document, the objectives), as well as direction and principles for action from the management viewpoint;
- necessary business requirements, legal and contractual requirements and other requirements relevant to the auditee;
- position and interface how the information security risk management is aligned with the organization's overall risk management including CSR, internal governance, financial control and safety etc;

- rationale for managing risks, such as that what primary assets should be considered as important to protect and which aspects of information security, i.e. either confidentiality, integrity or availability, should be evaluated most seriously when ISMS risk assessment is conducted; and
- approval and commitment of the top management.

Auditing the ISMS policy can be done by:

- confirming that the ISMS policy is produced as a document which includes signatures or seals indicating that the top management has established the policy;
- confirming through the relevant documents that procedures on establishing the policy (e.g. how the policy is authorized or reviewed within the organization) and rules for the procedures are defined, the rules are documented, and the methods for controlling the documents are specified;
- interviewing management to understand their approach and commitment to the organization's ISMS;
- evaluating, through the minutes and records of management review, the commitment and involvement of management in implementation, maintenance and improvement of the ISMS policy;
- assessing whether management has effectively communicated the ISMS policy, e.g. by focusing it on specific audiences, at all levels of the organization;
- conducting interviews with personnel in the ISMS scope to verify if they are aware of the importance of meeting information security objectives, conforming to the information security policy, and their information security responsibilities; and
- considering the information security policy (if available) and its relation to the ISMS policy.

Auditing ISMS objectives can be done by verifying that:

- organization's ISMS objectives have been defined, reflected in the ISMS policy, and aligned with the overall business objectives;
- ISMS controls and processes are identified and documented to meet the ISMS objectives;
- the objectives are adequately documented;
- ISMS objectives are suitably communicated to all levels of the organization; and
- the organization has assigned responsible personnel as resources required to achieve the objectives.

It is recommended that the auditor should examine the documented ISMS policy and objectives in the audit stage of document review;

ISMS policy and objectives are required to be reviewed and updated in response to the context change of the risk management. The auditor should confirm that continual improvements have been performed in relation to the business environment context.

The auditor should keep in mind that conformity to the ISMS policy and fulfilment of objectives can be measured in a quantitative or qualitative manner.

Risk assessment approach (4.2.1 c))

ISO/IEC 27001 requires that organizations define a risk assessment approach and Clauses 4.2.1 d) to f) specify elements of this approach. ISO/IEC 27001 does not state which risk assessment approach should be employed and any approach is acceptable as long as it meets the requirements in ISO/IEC 27001.

The auditor should verify that the risk assessment approach conforms to the requirements for risk assessment in ISO/IEC 27001 and is suitable for the organization and the overall risk management in place.

It should be confirmed that the risk assessment approach is implemented to identify risks in the business processes and activities and taking appropriate actions against the risks.

	ISO/IEC 27005 provides guidance on risk assessment and risk management. The auditor should be aware that there are quantitative and qualitative methods, or any combination of the two, for risk assessment, and that it is up to the organization to decide which approach to use. The processes and procedures for ISO/IEC 27001:2005 4.2.1 c) to j) are required to be defined, implemented and documented as a risk assessment approach in accordance with the management statement which is described in organization's ISMS policy (i.e. 4.2.1b) 4) criteria against which risk will be evaluated). The approach is defined as including how to deal with the compliance with legal and contractual requirements and other requirements relevant in relation to risks and assets that the organization should handle strategically in the context of business and risk assessment. At the audit, it should be confirmed that the approach is implemented and performed as required by ISO/IEC 27001:2005 4.2.1 b) to j). The auditor should confirm that the results of risk assessments by the risk assessment approach are comparable and reproducible. In other words, the auditor should confirm that the approach enables different personnel in charge of risk assessment to reach the same results regardless of whoever and whenever conducted risk assessment, provided that they have a certain level of competence in risk assessment and conducted the assessments to the same assets in accordance with the processes and procedures defined in the approach. And if a different result is brought up, it enables them to identify where and why the difference has occurred in the risk assessment. It is also necessary for the organization to have the approach be able to get to the same selection of controls for risk treatment if estimated risks are the same, i.e. with the same risk level and features (assets and security requirements). This confirmation should be performed by sampling on records of risk assessment report to trace both forward and backward along risk assessment process sequences, with on-site audits on assets in material. Criteria for accepting risks are often influenced by the organization's management policies, goals, technology, funds, relevant laws and regulations and interested parties, and they are eventually defined by the organization. It is therefore necessary for auditors to review with due attention, the effectiveness of the criteria in terms of those above entities, as well as confirming that they have been defined and exist. Auditors may refer to ISO/IEC 27005:2008 clause 7.2 for detailed interpretations of risk acceptance criteria.
A.2 Risk identification, analysis and evaluation, and risk treatment option identification and evaluation (ISO/IEC 27001 4.2.1d)～f))	
Audit Criteria	ISO/IEC 27001 4.2.1 d), e), f)
Relevant standards	ISO/IEC 27005 8.2, 8.3, 9, 10
Audit evidence	Audit evidence includes: • Inventory of assets; • Documents for the risk assessment methodology; • Risk assessment reports.
Audit practice guide	**Risk identification (4.2.1 d))**
	The auditor should review the asset inventory to confirm that all relevant important assets in the scope of the ISMS are included in the inventory, and accountable owners have been identified for all the assets. They should review the identifications of threats related to the assets, vulnerabilities exploited by the threats, and security failures caused by them, i.e. incident scenarios indicated in ISO/IEC 27005.

	Risk analysis and evaluation (4.2.1e))
	It is important to check that the risk assessment addresses all important assets in the ISMS scope and that the threat/vulnerability assessment in relation to the assets is tailored to the organization and does not just use pre-defined threat or vulnerability lists. It is also important to look for risks that are materially mis-stated or under-played, for example those where the corresponding controls are expensive or difficult to implement or where the risks have been misunderstood. The auditor should confirm on sampling, that all important assets listed in the asset inventory are included in the risk assessment and review the samples of the risk-evaluated incident scenarios to assess whether they reflect the business needs and impacts appropriately. Availability of competent personnel is important for a well-functioning ISMS. The auditor should assess the evidence that the medium and long term risks associated with the loss of availability of personnel have been adequately evaluated by the organization and reviewed to the most updated and that appropriate information security controls have been implemented to increase the resilience of the organization against these losses.
	Risk treatment options (4.2.1 f))
	The auditor should review the organization's selected risk treatment options. It should be reviewed that whether appropriate “treatments” (i.e. reduction through applying suitable controls, avoiding the risk, transferring the risk to third parties or knowingly accepting the risks if they fall within management's risk appetite) are specified for all identified risks. The auditor should look for gaps and other anomalies and check whether recent changes (e.g. new IT systems or business processes) have been suitably incorporated in the risk assessment and the risk treatment decisions.
A.3 Selection of control objectives and controls, approval of the proposed residual risks, management authorization, and Statement of Applicability (ISO/IEC 27001 4.2.1g) to j))	
Audit Criteria	ISO/IEC 27001 4.2.1 g) – j) , Annex A
Relevant standards	ISO/IEC 27005 9.1, 9.2, 10 ISO/IEC 27006 9.1.2
Audit evidence	Audit evidence includes: • Documents for the risk assessment methodology; • Risk assessment reports; • Documents describing the extent of reducing risks by the controls adopted (the results of risk assessment); • Records indicating approval of residual risks by the management (in particular, where residual risks are higher than the level defined in the criteria for accepting risks, their justification should be included.); • Records demonstrating authorization by the management on implementation and operation of the ISMS; • A statement of applicability.
Audit practice guide	**Selection of control objectives and controls (4.2.1 g))**
	For those information security requirements derived from the risk assessment and the risk treatment options selected to the requirements, the auditor should review that appropriate controls are selected and control objectives to be achieved are planned, with suitable samplings. The auditor should review that the selected controls and objectives conform to the information security requirements in the light of the control requirements defined in Annex A of ISO/IEC 27001 (as for interpretation of the control requirements in the Annex A, the best practices described as implementation guides in ISO/IEC 27002 may be good references). Any significant differences from Annex A requirements in control

	selection (e.g. if there are Annex A's control objectives and controls that are not adopted by the organization or additional objectives and controls selected from the outside of Annex A) should be identified and reviewed for rationale. In addition, the auditor should check that commonly adopted best practices for the relevant business sector have been considered in the control selection process. It should be checked that any information security requirements explicitly mandated by organization's policies, industry regulations, laws or contracts etc. are properly reflected in the documented control objectives and controls, and that risks have been reduced to clear the criteria for accepting risks. It should be confirmed that treatment of risks is repeatedly applied if the residual risks have not satisfied the criteria for accepting risks even after the adoption of controls.
	Approval of the proposed residual risks (4.2.1 h)) **Management authorization (4.2.1 i))**
	The auditor should briefly evaluate the residual information security risks and confirm that the organization has obtained management approval of the residual risks which remain after selecting controls for treatment of risks. It should be checked that management has formally considered and accepted the residual risks, the risks are within the organization's defined risk appetite, risk acceptance decisions are taken by sufficiently authorized levels of management of decision bodies, and where the levels of residual risks cannot be reduced below the acceptance criteria, the management decides to formally accept the risks and the reasons for the decision are recorded. In addition, the auditor should confirm that the management has authorized the implementation and operation of the ISMS, for example through a formal memorandum, project approval, letter of support from the CEO etc. It should be checked that this is not a mere formality and there is evidence that management really understands and supports the ISMS.
	Statement of Applicability (4.2.1 j))
	The auditor should review the organization's Statement of Applicability that documents and justifies the control objectives and controls, both those that are applicable and any that are not applicable. It is important that the Statement of Applicability demonstrates the link between the identified risks and the control objectives and controls that have been selected to reduce them. It is also important that justifications are given for controls being identified as not applicable The auditor should confirm that suitable entries exist for all control objectives and controls listed in Annex A of ISO/IEC 27001. The Statement of Applicability also needs to include the existing controls. It is necessary that the Statement of Applicability has been reviewed and endorsed/authorized by an appropriate level of management with the history records of created, approval, revision and updated, etc., as evidence.
A.4 Implementation and operation of the ISMS (4.2.2)	
Audit Criteria	ISO/IEC 27001 4.2.2
Relevant standards	ISO/IEC 27001 Annex A ISO/IEC 27002 ISO/IEC 27005 8.2.1.4, 9.1
Audit evidence	Audit evidence includes: • Risk treatment plan and progress records on the plan projects; • Documented procedures and records for control effectiveness measurements.

Audit practice guide	The auditor should confirm that the organization has formulated and implemented a risk treatment plan with the identified risk treatment options. It is important to confirm that: • the risk treatment plan has been implemented, taking account of priorities and responsibilities, as defined; • sufficient resources are allocated to support the operation of the ISMS (see also Clause C.9 below) • priorities and timing for implementing respective risk treatment are clearly identified; • funds, roles and responsibilities for the risk treatment are identified; and • the Risk Treatment Plan is used and updated proactively as an information security management tool. The auditor should review the ISMS as implemented and operated against the documented ISMS requirements by sampling of controls (see 4.2.1g) and Annex A of ISO/IEC 27001) on their implementation and performance. It is necessary to look for evidence supporting or refuting the correlation between documented risks and planned and implemented controls. The auditor should confirm that the purpose and the way to measure the effectiveness of selected controls have been clearly defined. It is important to be able to check whether the controls actually reduce the risks or impacts of incidents in the method to measure the effectiveness of controls. (ISO/IEC 27005 8.2.1.4) When auditing the ISMS measurements, note that measurements can be achieved in a number of ways, some more complex than others. The auditor needs to be aware that although there is guidance on ISMS measurements available, the requirements of ISO/IEC 27001 will be met as long as the criteria for producing comparable and reproducible results of assessment of control effectiveness are defined and accepted by management. It is also important to ensure that the ISMS measurements meet the business requirements of the organization, taking into account the results of the risk assessment and treatment process. Effective measurements ensure that the control is effectively reducing the related risks. When auditing the operation of the ISMS, the auditor should evaluate how the organization ensures the effectiveness of controls. To this end the auditor should assess the extent and sufficiency of ISMS measurements.
A.5 ISMS monitoring and review (ISO/IEC 27001 4.2.3)	
Audit Criteria	ISO/IEC 27001 4.2.3
Relevant standards	ISO/IEC 27005 12.1, 12.2
Audit evidence	Audit evidence includes: • Security events reports / incidents reports; • Documents for management reviews (inputs and outputs); • Definition (procedures) of measuring the effectiveness of the controls, and records on measuring and assessing the controls; • Records on using the measurement (including measures for strengthening the controls, records of corrective and preventive actions, and a risk treatment plan); • Documents containing information about information assets, risk analysis and assessment, risk treatment plan, and a statement of applicability; • An annual plan for information security.

Audit practice guide	The auditor should review the ISMS monitoring and review processes using evidence such as plans, minutes of review meetings, management review/internal ISMS audit reports, breach/incident reports etc. The auditor should assess the extent to which processing errors, security breaches and other incidents are detected, reported and addressed. It is important to determine whether and how the organization is effectively and proactively reviewing the implementation of the ISMS to ensure that the security controls identified in the Risk Treatment Plan, policies etc. are actually implemented and are in fact in operation. The auditor should also review ISMS measurements and their use to drive continual ISMS improvements. It should also be confirmed that changes to be considered (4.2.3 d) 1) to 6) in ISO/IEC 27001) are reflected in the processes for identifying, analyzing, evaluating and treating the risks. In addition, it should be confirmed that the ISMS documents and records related to risk assessment have been updated. The auditor should take particular care over auditing the ISMS monitoring and review processes. These will be quite different dependent on type and size of organization, but the activities that need to be demonstrated by the organization are clearly laid out in ISO/IEC 27001. Of particular concern to auditors is the issue of change and whether the organization has considered internal and/or external changes to its operations, and whether those changes will have had an effect on its ISMS.
A.6 ISMS maintaining and improvement (ISO/IEC 27001 4.2.4 and 8)	
Audit Criteria	ISO/IEC 27001 4.1, 4.2.4, 8
Relevant standards	ISO/IEC 27001 4.2.4 and 8
Audit evidence	Audit evidence includes: • Identified improvements reports from the activities defined in 27001 4.2.3; • Non-conformity reports; • Corrective/preventive action reports; • Security event reports/incident reports; • Documented procedures and controls in support of the ISMS; • Records of ISMS operation; • Risk assessment reports; • Procedures for corrective and preventive action; • Statement of Applicability.
Audit practice guide	**ISMS maintaining and improvement (4.2.4)** The identified improvements specified in 4.2.4 a) of ISO/IEC 27001 indicate the improvements which have been identified through monitoring and reviewing processes in 4.2.3 of ISO/IEC 27001. The auditor should review the means and records by which the need for ISMS improvements is determined and the way how the improvements are implemented. The auditor should also look for evidence in the form of management memos, minutes, reports, emails etc. documenting the need for improvements, authorizing them and making them happen. ISMS auditors should look for tangible evidence of improvement in policies, procedures, methods and controls, new risk assessments, IS policy reviews and changes, new business activities including new interested parties, maintenance (not only in IT but also facilities and lifetime estimates for installations), capacity and incident management activities, changes to information handling and transportation procedures as well as changes in legal, technical and security compliance for external parties.

	Thus, at the audit, It should also be confirmed that procedures and processes to implement the improvements conform to requirements specified in 4.2.4 b) to d) of ISO/IEC 27001.
	ISMS improvement (8)
	Continual improvement (8.1)
	The auditor should verify how the organization has determined whether the ISMS can be improved, how it has evaluated the associated risks, and how this relates to the identified security requirements and the monitoring of the ISMS performance. The auditor has to verify how the overall organization's objectives have been translated into internal information security requirements throughout the appropriate processes, and how these requirements are communicated and monitored. So, the auditor should look for evidence that the organization is analysing data from the ISMS monitoring, and is then taking the results forward for evaluating the ISMS effectiveness and improving the ISMS, where necessary. The auditor should confirm that the improvement objectives and priorities are consistent with the ISMS objectives. However, It should be concluded that the organization that does not have a policy and objectives relating to continual improvement is clearly not complying with the standard. If the management has set a (realistic) objective for improvements, and there is no evidence of improvement, this information should be fed back into the management review so that management can decide what type of action is appropriate - for example, re-adjusting the objective or providing other means to impact on the process. If the organization uses performance statistics (e.g. reduction of the number of certain security incidents) to measure improvements the auditor should carefully evaluate if those statistics actually relate to identified risks or if the selection was based on the ease of calculation.
	Corrective action (8.2)
	The auditor should obtain and review information relating to ISMS corrective actions such as reports and action plans from ISMS management review(s) or audits (see ISO/IEC 27001 Section 7.3), ISMS change requests, budget/investment proposals and business cases etc. The auditor should seek evidence that the ISMS is in fact being materially improved as a result of the feedback - check the documentation relating to closure of action plan items etc. to confirm whether nonconformities and their root causes are actually being effectively resolved by management within reasonable timescales. Often there are the cases that remedies are taken to nonconformities but the actions to prevent their recurrences are not yet taken because the root causes analysis has been failed. With corrective action reports, the auditor should review the records of the corrective actions and confirm whether the recorded actions are effective through conducting on-site observation as applicable. In terms of ISMS risk management, the root cause analysis should be performed to: • identify whether it is due to the fact that the risks are not identified; • if the risks are identified, check whether controls (measures) to the risks are applied; • if the risks are identified and controls are applied to the risks, check whether the applied controls are appropriate for the risks; and • if the risks are identified and the appropriate controls are applied to the risks, verify whether the controls are implemented effectively or performed as expected.

	Either of or combination of the cases above would be the cause to nonconformities. In the context of the risk management, the occurrences of nonconformity can be considered as the risks being exposed, and potential nonconformities can be considered as the risks predicted. The auditor should verify and confirm whether the root cause of nonconformities are identified with detailed analysis described as the above, and whether the actions taken to the nonconformities are appropriate, with the records and observed facts on site as possible.
	Preventive action (8.3)
	In addition to making ISMS improvements resulting from actual nonconformities previously identified, the auditor should determine whether the organization takes a more proactive stance towards addressing potential improvements, emerging or projected new requirements etc. The auditor should seek evidence of ISMS changes (such as adding, changing or removing information security controls) in response to the identification of significantly changed risks. The following items can be considered when auditing preventive actions: 1.) How the organization determines potential nonconformities and their causes. Typical examples include: • Identification of new or changed risks through update of the risk assessment (ISO/IEC 27001 4.2.3 d) and 8.3); • Trend analysis for ISMS characteristics. A worsening trend might indicate that if no action is taken, a nonconformity could occur; • Alarms to provide early warning of approaching “out-of-control” operating conditions; • Incident monitoring and analysing trends of incidents; • Evaluation of nonconformities that have occurred in similar circumstances, but for other parts of the ISMS, or other parts of the organization, or even in other organizations; • The planning process for both predictable situations (e.g. due to expansion, maintenance, or personnel changes) and for unpredictable situations (e.g. changes in legislation, naturally occurring problems such as hurricanes, earthquakes, floods etc.). 2.) How the organization determines what action is required, and how it is implemented. An auditor should look for evidence that: • the organization has analyzed the causes of potential nonconformities (use of cause and effect diagrams and other information security tools may be appropriate for this); • the required actions are deployed in all relevant parts of the organization, and in a timely manner; • there are clear definitions of the responsibilities for the identification, evaluation, implementation and review of preventive actions; and • adequate training is given for new or changed controls. 3.) An auditor should confirm that: • appropriate records are kept; • the records are a true reflection of the results; • the records are being controlled in accordance with ISO/IEC 27001:2005, Clause 4.3.3. 4.) For a review of the preventive actions taken, an auditor should consider whether: • the actions were effective (i.e. was a non-conformity prevented from occurring and were there any additional benefits);

	• there is a need to continue with the preventive actions the way they are; • the preventive actions should be changed, or whether it is necessary to plan new actions.
A.7 ISMS documentation (ISO/IEC 27001 4.3)	
Audit Criteria	ISO/IEC 27001 4.3.1 to 4.3.3
Relevant standards	—
Audit evidence	Audit evidence includes: • The ISMS documentation described in 27001 4.3.1 a) to i).
Audit practice guide	**Documentation requirements (4.3)**
	ISMS documentation (4.3.1)
	It is important to identify the documentation requirements specified in the ISMS. The auditor should consider the requirements in ISO/IEC 27001, Clause 4.3.1 and several places indicated in Clause 5 to 8, in addition to Annex A controls, and also the requirements specified in the ISMS documentation by the organization. The auditor should request and acquire the information on the auditee's operating processes, interview the personnel at all levels (including administrative personnel, process owners and operators) and observe their activities and behaviour and the process performance to confirm that the ISMS implementation and performance on-site conform to the documented and specified requirements. The necessity for any documentation should be evaluated in the light of the observed need for consistency, the importance of the information it contains and the role that any documentation could play in avoiding any significant, identified risks.
	ISMS documentation control (4.3.2)
	The auditor should check for the presence of, and compliance with, a documented procedure for controlling updates to ISMS documentation, policies, procedures, records etc. The auditor should also determine whether ISMS documentation changes are formally controlled e.g. changes are reviewed and pre-approved by management, and are promulgated to all users of the ISMS documentation e.g. by updating a definitive reference set of materials maintained on the corporate intranet and/or explicitly notifying all applicable users.
	ISMS records (4.3.3)
	The auditor should evaluate the controls protecting important ISMS records such as various information security review and audit reports, action plans, formal ISMS documents (including changes to same), visitors' books, access authorization/change forms etc. It is necessary to review the adequacy of controls over the identification, storage, protection, retrieval, retention time and disposition of such records, particularly in situations where there are legal and contractual requirements and other requirements relevant to the implementation of an ISMS in compliance with ISO/IEC 27001 (e.g. to protect personal data).

<table>
<tr><th colspan="2">A.8 Management responsibility (ISO/IEC 27001 5)</th></tr>
<tr><td>Audit Criteria</td><td>ISO/IEC 27001 5.1, 5.2.1 and 5.2.2</td></tr>
<tr><td>Relevant standards</td><td>ISO/IEC 27006 9.2.3.2.2i)
ISO/IEC 27001 4.2.1 b)5)、Annex A.5.1.1、A.6.1.1
ISO/IEC 17021 9.2.3.2 f)
ISO/IEC 27006 9.2.3.2.2 f)
ISO/IEC 27005 9.2</td></tr>
<tr><td>Audit evidence</td><td>Audit evidence includes:
ISMS policy with date of approval, signatures, etc.;
Review records of the ISMS policy;
Security plans/schedules for the ISMS activities, e.g. risk treatment plan, education and training programme/plan, internal audit programme/plan, etc.;
Management review minutes with input/output documentations, minutes of the organization’s information security committee, etc;
Documents of roles and responsibilities;
Internal audits report;
Risk assessment report;
Management interview;
Records of approval of residual risks, he approval of the risk treatment plan, records of management reviews, decision of budgets on the business plan, and results of approval of requests for decisions;
Records of reviews of PDCA activities and controls;
Competence criteria;
Human resources and competence records;
Training programme/plans;
Training reports and records.</td></tr>
<tr><td rowspan="4">Audit practice guide</td><td>Management commitment (5.1)</td></tr>
<tr><td>The auditor should review the extent of management commitment to information security, using evidence such as:
formal management approval of the ISMS policy;
management acceptance of ISMS objectives and implementation plans, along with the allocation of adequate resources and assignment of suitable priorities to the associated activities (see also 5.2.1);
clear roles and responsibilities for information security including a process for allocating and accepting accountability for the proper protection of valuable information assets;
management memoranda, emails, minutes, presentations, briefings, job descriptions, etc. expressing support for and commitment to the ISMS;
risk acceptance criteria and their formal acceptance, risk appetite etc. relating to information security risks; and
the scoping, resourcing and initiation of internal audits and management reviews of the ISMS.</td></tr>
<tr><td>Allocation of ISMS resources (5.2.1)</td></tr>
<tr><td>The auditor should verify that the resources needed to implement, maintain and improve the ISMS are adequately managed. This means that the organization needs to identify, plan, make available, use, monitor and change the appropriate resources as required.

It is recommended that the management of resources is not audited in isolation. Irrespective of the way the organization is structured and identifies its processes, auditors should be able to verify the adequacy and effective management of the resources to achieve planned results. It is important for auditors to verify whether the organization has</td></tr>
</table>

	evaluated past and present performance (e.g. using cost-benefit analysis, risk assessment) when deciding what resources are to be allocated. Management of resources can be evaluated by interviews with management and other responsible personnel to check that suitable processes are in place. This needs, however, to be supported by objective evidence collected throughout the audit. Evidence can be obtained at different stages of the audit – reviewing inputs, process performance and outputs. This should be carried out when auditing all the processes and related system and process documentation, such as: • management commitment and responsibilities; • management review process; • ISMS processes including the risk management, corrective and preventive actions and continual improvement; • job description; and • budget and time records for ISMS specific activities. Auditors should avoid making subjective judgements on the adequacy of the resources allocated by the organization and should limit their role to the evaluation of the effectiveness of the resource management process.
	ISMS awareness and training (5.2.2)
	The auditor should review the training of those specifically involved in operating the ISMS, and general information security awareness activities targeting all employees. It should be checked whether necessary competencies and training/awareness requirements for information security professionals and others with specific roles and responsibilities are explicitly identified, and whether information security training and awareness needs supported by adequate budgets. The auditor should review training evaluation reports etc. and seek evidence to confirm that any necessary improvement actions have in fact been taken. It is necessary to check by sampling that employee HR records note ISMS-related training etc. (where applicable). The auditor should assess the general level of information security awareness by surveying/sampling, or review the results of surveys/samples conducted as part of the ISMS. To satisfy the competence/effectiveness requirements of ISO/IEC 27001, an organization will typically need to do several things: • identify what competencies are required by personnel performing work which affects information security; • identify which personnel already performing the work have the required competencies; • decide what additional competencies are required; • decide how these additional competencies are to be obtained – training of personnel (external or internal), theoretical or practical training, hiring of new competent personnel, assignment of existing competent personnel to different work; • review the effectiveness of actions taken to satisfy competence needs; and • periodically review competence of personnel. Throughout the process, the organization is required to maintain appropriate records of education, training, skills and experience. However, ISO/IEC 27001 does not specify how the process will be established or the exact nature of the records to be maintained. 1.) In auditing an organization's compliance with the competence and training evaluation requirements, an auditor would typically be seeking evidence that the following issues are addressed: An organization needs to identify what competencies are required by personnel performing work effecting the information security.

	The objective of the auditor should be to determine whether there is a systematic approach in place to identify these competencies and to verify that the approach is effective. The outcome of the process may be a list, register, database, human resources plan, competencies development plan, contract, project or product plan, etc. Discussions could initially be held with management to ensure they understand the importance of identifying the competencies required. These may also be a potential source of information regarding new or changed activities or processes, which may lead to different competency requirements in the organization. A review of competencies might also be needed when a new tender or contract is being considered. Evidence of this could be found in related records. Competence requirements may be included in contract documents where the activities of subcontractors can have an impact on processes and/or information security. Auditors need to determine whether the organization has identified new or changed competence needs, e.g. during surveillance audits. 2.) The auditor should review that competent personnel are assigned to those work place activities necessary to control information security. The auditor should verify that some form of evaluation process is in place to ensure that the competencies are appropriate to the organization's activities, and that the personnel selected as competent are demonstrating appropriate competencies. Also, the process should ensure that any deficiencies are being acted upon and the effectiveness of personnel is being measured. It is necessary to verify that the activities that affect information security are performed by persons selected as competent. Evidence may be obtained throughout the audit with an emphasis on those processes, activities, task and products where human intervention may have the greatest impact. The auditor may review job descriptions, testing or inspection activities, monitoring activities, records of management reviews, definition of responsibilities and authorities, nonconformity records, audit reports, customer complaints, processes validation records etc. 3.) The organization needs to evaluate the effectiveness of the actions taken to satisfy the competence needs The organization may use a number of techniques including role-play, peer review, observation, reviews of training and employment records and/or interviews (see ISO 19011:2011, Table 2, for further examples). The appropriateness of a particular evaluation method will depend on many factors. For example, training records could be viewed to verify that a training course had been successfully completed (but note, this alone would not provide evidence that the trainee is competent). However, this same method would not be acceptable to evaluate whether an auditor performed satisfactorily during an audit. Instead, this may require observation, peer review, interviews, etc. The organization may need to demonstrate the attainment of competence of its personnel through a combination of education, training and/or work experience. 4.) Maintenance of competence. The auditor needs to verify that some form of effective monitoring process is in place and being acted upon. Ways of doing this include a continuing professional development process (such as the one described in ISO 19011, Clause 7.4), regular appraisals of personnel and their performance, or the regular inspection, testing or auditing of product or system for which individuals or groups are responsible. Ongoing changes in competence requirements may indicate that an organization is proactive in maintaining personnel performance levels.
A.9 Internal ISMS audits and ISMS management review (ISO/IEC 27001 6 and 7) - This clause provides guidance to external auditing or self check or peer assessment guidance to internal auditing.	

Audit Criteria	ISO/IEC 27001 6, 7
Relevant standards	ISO/IEC 27005 7. 9 ISO/IEC 27006 9.1.2, 9.1.4, 9.2.3.2.2 ISO/IEC 17021 9.2.3.2, 9.3.2.1
Audit evidence	Audit evidence includes: • Internal audits programme, plans, reports and records; • Management review minutes with input and output documents; • Risk assessment reports.
Audit practice guide	**Internal ISMS audits (6)**
	The auditor should review the organization's internal audits of the ISMS, using ISMS audit programmes, plans, audit reports, action plans *etc*. It should be verified that responsibilities for conducting Internal ISMS audits are formally assigned to competent, adequately trained auditors. The auditors should determine the extent to which the internal ISMS audits confirm that the ISMS meets its requirements defined in ISO/IEC 27001 and legal and contractual requirements and other requirements, and organizational ISMS requirements specified through the risk assessment process. ISO/IEC 27001 Clauses 6a) – 6d) can be extended to checklists to support the audit. The auditor should also check that agreed action plans, corrective actions, etc. are being addressed and verified within the agreed timescales, paying particular attention to any overdue actions for current examples. The organization should be able to maximize the use of available resources during the conduct of internal ISMS audit activities. There should be evidence that the organization: • has identified the competence requirements for its internal ISMS auditors; • has provided appropriate training; • has in place a process for monitoring the performance of its internal ISMS auditors and audit teams; and • includes personnel on its audit teams that have appropriate sector specific knowledge (so that they are able to identify where a change in a particular process or activity might lead to a significant consequence for information security). It should be ascertained that the organization has planned its internal ISMS audits, and that its audit methods have been defined, in order to ensure the effective and efficient use of resources. This should also help to ensure that the inherent risks of audit failure in the audit process, and to audit outcomes, are minimised. The organization should have a process for utilizing past audit results in the planning of future internal ISMS audits. The auditor should verify that the organization use such information when establishing the audit frequency of such processes and activities. By taking the above factors into account, and by examining whether the internal ISMS audit process is leading to any tangible improvements to the ISMS, the ISMS auditor should be able to form a judgement on whether the organization has implemented an effective internal ISMS audit programme.The ISMS auditor should also be able to form a judgement as to whether the outcome of internal ISMS audits does provide adequate evidence to be used as part of the improvement process of the ISMS.
	Management review of the ISMS (7)
	Auditing the ISMS management review (7.1)
	ISO/IEC 27001 requires management to review the organization's ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness. Determine when management has previously reviewed the ISMS, and when

it next plans to do so. The frequency of reviews should be defined, e.g. in the ISMS policy or ISM policy manual.

The review could be carried out at a separate meeting but this is not a requirement of the standard. There are many ways in which management can review the ISMS, such as receiving and reviewing reports, electronic communication or as part of regular management meetings where issues such as budgets and targets are also discussed.

The management review process should not be an exercise carried out solely to satisfy the requirements of the standard and the auditors; it should be an integral part of the organization's business management process. Overall management review is a complex process carried out at various levels in the organization. It should always be a two-way process, generated by top management with inputs from all levels in the organization. These activities could vary from daily, weekly, monthly, organizational unit meetings to simple discussions or reports.

Auditors should look for evidence that the inputs and outputs of the management review process are relevant to the organization's size and complexity and that they are used to improve the ISMS. Auditors should also consider how the organization's management is structured and how the management review process is used within this structure.

Records of management reviews are required but the format of these is not specified. Minutes of meetings are the most common type of record, but electronic records, statistical charts, presentations etc. could be acceptable types of records. It is important to ensure that there is evidence to demonstrate that consideration has been given to all the issues listed in ISO/IEC 27001:2005 Clause 7, even where it is decided that no action is necessary.

The management review process might also include elements of ISMS planning where changes to processes and systems are being considered. Where this is the case, the auditors should review whether or not the following points have been considered:

- Are proposed changes evaluated before implementation?
- In preparing strategic plans, are issues related to the ISMS considered?
- Are the controls needed identified before changes are implemented, e.g. the outsourcing of a process is started.

Management review input (7.2)

ISO/IEC 27001 Clause 7.2 specifies the inputs to the management review process and these topics need to be included. However, these are not the only subjects that can be ncluded in a review. They might not be addressed individually or simultaneously but as part of an overall review of the business. Auditors should be aware that inputs could be in many forms such as reports, trend charts and so on.

By reviewing management reports, minutes, and other records, and/or by interviewing those who were involved, it should be checked what went in to the previous management review(s) (ISO/IEC 27001 identifies nine items such as the results of other audits/reviews, feedback and improvement suggestions, information on vulnerabilities and threats etc.). It is necessary to assess the extent to which management played an active part and was fully engaged in the review(s).

Management review output (7.3)

ISO/IEC 27001 Clause 7.3 specifies the outputs to the management review process and any decisions and actions related to these topics a) – e) need to be included. The auditor should check the outputs of any previous management review(s) including key management decisions, action plans and records relating to the confirmation that agreed actions were duly carried out. As output from the management review process, there should be evidence of decisions regarding to the a) – e) such as:

	• change of ISMS policy and objectives; • plans and possible actions for improvements; • change of resources; • revised business plans; • budgets; • revised statement of applicability; and • revised control measurements. Output is not only related to improvements or changes but could include decisions on other important issues such as plans to introduce new technologies, systems or products. If necessary, confirm that closed actions have in fact been properly completed, paying particular attention to any actions that were not completed promptly or on time.

Bibliography

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

[2] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[3] ISO/IEC 27003:2010, *Information technology — Security techniques — Information security management system implementation guidance*

[4] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*

[5] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

[6] ISO/IEC 27006:2007, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[7] IAF MD1:2007, *IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling*, International Accreditation Forum

ICS 35.040

Price based on 27 pages