BS EN ISO 19011:2011

BSI Standards Publication

Guidelines for auditing management systems (ISO 19011:2011)

National foreword

This British Standard is the UK implementation of EN ISO 19011:2011. It supersedes BS EN ISO 19011:2002 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee AUS/1, Revision of ISO 19011.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 66496 0

ICS 03.120.10; 13.020.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2011.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 19011

October 2011

ICS 03.120.10; 13.020.10

Supersedes EN ISO 19011:2002

English Version

Guidelines for auditing management systems (ISO 19011:2011)

Lignes directrices pour l'audit des systèmes de management (ISO 19011:2011)

Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2011)

This European Standard was approved by CEN on 11 October 2011.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO 19011:2011: E

Foreword

This document (EN ISO 19011:2011) has been prepared by Technical Committee ISO/TC 176 "Quality management and quality assurance".

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2012, and conflicting national standards shall be withdrawn at the latest by April 2012.

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

This document supersedes EN ISO 19011:2002.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Endorsement notice

The text of ISO 19011:2011 has been approved by CEN as a EN ISO 19011:2011 without any modification.

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Principles of auditing ... **4**

5 Managing an audit programme ... **5**
5.1 General ... **5**
5.2 Establishing the audit programme objectives ... **6**
5.3 Establishing the audit programme ... **7**
5.4 Implementing the audit programme ... **10**
5.5 Monitoring the audit programme ... **13**
5.6 Reviewing and improving the audit programme ... **14**

6 Performing an audit ... **14**
6.1 General ... **14**
6.2 Initiating the audit ... **15**
6.3 Preparing audit activities ... **16**
6.4 Conducting the audit activities ... **18**
6.5 Preparing and distributing the audit report ... **23**
6.6 Completing the audit ... **24**
6.7 Conducting audit follow-up ... **24**

7 Competence and evaluation of auditors ... **24**
7.1 General ... **24**
7.2 Determining auditor competence to fulfil the needs of the audit programme ... **25**
7.3 Establishing the auditor evaluation criteria ... **29**
7.4 Selecting the appropriate auditor evaluation method ... **29**
7.5 Conducting auditor evaluation ... **29**
7.6 Maintaining and improving auditor competence ... **29**

Annex A (informative) **Guidance and illustrative examples of discipline-specific knowledge and skills of auditors** ... **31**

Annex B (informative) **Additional guidance for auditors for planning and conducting audits** ... **37**

Bibliography ... **44**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 shall not be held responsible for identifying any or all such patent rights.

ISO 19011 was prepared by Technical Committee ISO/TC 176, *Quality management and quality assurance*, Subcommittee SC 3, *Supporting technologies*.

This second edition cancels and replaces the first edition (ISO 19011:2002), which has been technically revised.

The main differences compared with the first edition are as follows:

— the scope has been broadened from the auditing of quality and environmental management systems to the auditing of any management systems;

— the relationship between ISO 19011 and ISO/IEC 17021 has been clarified;

— remote audit methods and the concept of risk have been introduced;

— confidentiality has been added as a new principle of auditing;

— Clauses 5, 6 and 7 have been reorganized;

— additional information has been included in a new Annex B, resulting in the removal of help boxes;

— the competence determination and evaluation process has been strengthened;

— illustrative examples of discipline-specific knowledge and skills have been included in a new Annex A;

— additional guidelines are available at the following website: www.iso.org/19011auditing.

Introduction

Since the first edition of this International Standard was published in 2002, a number of new management system standards have been published. As a result, there is now a need to consider a broader scope of management system auditing, as well as providing guidance that is more generic.

In 2006, the ISO committee for conformity assessment (CASCO) developed ISO/IEC 17021, which sets out requirements for third party certification of management systems and which was based in part on the guidelines contained in the first edition of this International Standard.

The second edition of ISO/IEC 17021, published in 2011, was extended to transform the guidance offered in this International Standard into requirements for management system certification audits. It is in this context that this second edition of this International Standard provides guidance for all users, including small and medium-sized organizations, and concentrates on what are commonly termed “internal audits” (first party) and “audits conducted by customers on their suppliers” (second party). While those involved in management system certification audits follow the requirements of ISO/IEC 17021:2011, they might also find the guidance in this International Standard useful.

The relationship between this second edition of this International Standard and ISO/IEC 17021:2011 is shown in Table 1.

Table 1 — Scope of this International Standard and its relationship with ISO/IEC 17021:2011

Internal auditing	External auditing	
	Supplier auditing	Third party auditing
Sometimes called first party audit	Sometimes called second party audit	For legal, regulatory and similar purposes For certification (see also the requirements in ISO/IEC 17021:2011)

This International Standard does not state requirements, but provides guidance on the management of an audit programme, on the planning and conducting of an audit of the management system, as well as on the competence and evaluation of an auditor and an audit team.

Organizations can operate more than one formal management system. To simplify the readability of this International Standard, the singular form of “management system” is preferred, but the reader can adapt the implementation of the guidance to their own particular situation. This also applies to the use of “person” and “persons”, “auditor” and “auditors”.

This International Standard is intended to apply to a broad range of potential users, including auditors, organizations implementing management systems, and organizations needing to conduct audits of management systems for contractual or regulatory reasons. Users of this International Standard can, however, apply this guidance in developing their own audit-related requirements.

The guidance in this International Standard can also be used for the purpose of self-declaration, and can be useful to organizations involved in auditor training or personnel certification.

The guidance in this International Standard is intended to be flexible. As indicated at various points in the text, the use of this guidance can differ depending on the size and level of maturity of an organization’s management system and on the nature and complexity of the organization to be audited, as well as on the objectives and scope of the audits to be conducted.

This International Standard introduces the concept of risk to management systems auditing. The approach adopted relates both to the risk of the audit process not achieving its objectives and to the potential of the audit to interfere with the auditee’s activities and processes. It does not provide specific guidance on the organization’s risk management process, but recognizes that organizations can focus audit effort on matters of significance to the management system.

This International Standard adopts the approach that when two or more management systems of different disciplines are audited together, this is termed a “combined audit”. Where these systems are integrated into a single management system, the principles and processes of auditing are the same as for a combined audit.

Clause 3 sets out the key terms and definitions used in this International Standard. All efforts have been taken to ensure that these definitions do not conflict with definitions used in other standards.

Clause 4 describes the principles on which auditing is based. These principles help the user to understand the essential nature of auditing and they are important in understanding the guidance set out in Clauses 5 to 7.

Clause 5 provides guidance on establishing and managing an audit programme, establishing the audit programme objectives, and coordinating auditing activities.

Clause 6 provides guidance on planning and conducting an audit of a management system.

Clause 7 provides guidance relating to the competence and evaluation of management system auditors and audit teams.

Annex A illustrates the application of the guidance in Clause 7 to different disciplines.

Annex B provides additional guidance for auditors on planning and conducting audits.

Guidelines for auditing management systems

1 Scope

This International Standard provides guidance on auditing management systems, including the principles of auditing, managing an audit programme and conducting management system audits, as well as guidance on the evaluation of competence of individuals involved in the audit process, including the person managing the audit programme, auditors and audit teams.

It is applicable to all organizations that need to conduct internal or external audits of management systems or manage an audit programme.

The application of this International Standard to other types of audits is possible, provided that special consideration is given to the specific competence needed.

2 Normative references

No normative references are cited. This clause is included in order to retain clause numbering identical with other ISO management system standards.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
audit
systematic, independent and documented process for obtaining **audit evidence** (3.3) and evaluating it objectively to determine the extent to which the **audit criteria** (3.2) are fulfilled

NOTE 1 Internal audits, sometimes called first party audits, are conducted by the organization itself, or on its behalf, for management review and other internal purposes (e.g. to confirm the effectiveness of the management system or to obtain information for the improvement of the management system). Internal audits can form the basis for an organization's self-declaration of conformity. In many cases, particularly in small organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited or freedom from bias and conflict of interest.

NOTE 2 External audits include second and third party audits. Second party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf. Third party audits are conducted by independent auditing organizations, such as regulators or those providing certification.

NOTE 3 When two or more management systems of different disciplines (e.g. quality, environmental, occupational health and safety) are audited together, this is termed a combined audit.

NOTE 4 When two or more auditing organizations cooperate to audit a single **auditee** (3.7), this is termed a joint audit.

NOTE 5 Adapted from ISO 9000:2005, definition 3.9.1.

3.2
audit criteria
set of policies, procedures or requirements used as a reference against which **audit evidence** (3.3) is compared

NOTE 1 Adapted from ISO 9000:2005, definition 3.9.3.

NOTE 2 If the audit criteria are legal (including statutory or regulatory) requirements, the terms "compliant" or "non-compliant" are often used in an **audit finding** (3.4).

3.3
audit evidence
records, statements of fact or other information which are relevant to the **audit criteria** (3.2) and verifiable

NOTE Audit evidence can be qualitative or quantitative.

[ISO 9000:2005, definition 3.9.4]

3.4
audit findings
results of the evaluation of the collected **audit evidence** (3.3) against **audit criteria** (3.2)

NOTE 1 Audit findings indicate conformity or nonconformity.

NOTE 2 Audit findings can lead to the identification of opportunities for improvement or recording good practices.

NOTE 3 If the audit criteria are selected from legal or other requirements, the audit finding is termed compliance or non-compliance.

NOTE 4 Adapted from ISO 9000:2005, definition 3.9.5.

3.5
audit conclusion
outcome of an **audit** (3.1), after consideration of the audit objectives and all **audit findings** (3.4)

NOTE Adapted from ISO 9000:2005, definition 3.9.6.

3.6
audit client
organization or person requesting an **audit** (3.1)

NOTE 1 In the case of internal audit, the audit client can also be the **auditee** (3.7) or the person managing the audit programme. Requests for external audit can come from sources such as regulators, contracting parties or potential clients.

NOTE 2 Adapted from ISO 9000:2005, definition 3.9.7.

3.7
auditee
organization being audited

[ISO 9000:2005, definition 3.9.8]

3.8
auditor
person who conducts an **audit** (3.1)

3.9
audit team
one or more **auditors** (3.8) conducting an **audit** (3.1), supported if needed by **technical experts** (3.10)

NOTE 1 One auditor of the audit team is appointed as the audit team leader.

NOTE 2 The audit team may include auditors-in-training.

[ISO 9000:2005, definition 3.9.10]

3.10
technical expert
person who provides specific knowledge or expertise to the **audit team** (3.9)

NOTE 1 Specific knowledge or expertise is that which relates to the organization, the process or activity to be audited, or language or culture.

NOTE 2 A technical expert does not act as an **auditor** (3.8) in the audit team.

[ISO 9000:2005, definition 3.9.11]

3.11
observer
person who accompanies the **audit team** (3.9) but does not audit

NOTE 1 An observer is not a part of the **audit team** (3.9) and does not influence or interfere with the conduct of the **audit** (3.1).

NOTE 2 An observer can be from the **auditee** (3.7), a regulator or other interested party who witnesses the **audit** (3.1).

3.12
guide
person appointed by the **auditee** (3.7) to assist the **audit team** (3.9)

3.13
audit programme
arrangements for a set of one or more **audits** (3.1) planned for a specific time frame and directed towards a specific purpose

NOTE Adapted from ISO 9000:2005, definition 3.9.2.

3.14
audit scope
extent and boundaries of an **audit** (3.1)

NOTE The audit scope generally includes a description of the physical locations, organizational units, activities and processes, as well as the time period covered.

[ISO 9000:2005, definition 3.9.13]

3.15
audit plan
description of the activities and arrangements for an **audit** (3.1)

[ISO 9000:2005, definition 3.9.12]

3.16
risk
effect of uncertainty on objectives

NOTE Adapted from ISO Guide 73:2009, definition 1.1.

3.17
competence
ability to apply knowledge and skills to achieve intended results

NOTE Ability implies the appropriate application of personal behaviour during the audit process.

3.18
conformity
fulfilment of a requirement

[ISO 9000:2005, definition 3.6.1]

3.19
nonconformity
non-fulfilment of a requirement

[ISO 9000:2005, definition 3.6.2]

3.20
management system
system to establish policy and objectives and to achieve those objectives

NOTE A management system of an organization can include different management systems, such as a quality management system, a financial management system or an environmental management system.

[ISO 9000:2005, definition 3.2.2]

4 Principles of auditing

Auditing is characterized by reliance on a number of principles. These principles should help to make the audit an effective and reliable tool in support of management policies and controls, by providing information on which an organization can act in order to improve its performance. Adherence to these principles is a prerequisite for providing audit conclusions that are relevant and sufficient and for enabling auditors, working independently from one another, to reach similar conclusions in similar circumstances.

The guidance given in Clauses 5 to 7 is based on the six principles outlined below.

a) **Integrity:** the foundation of professionalism

Auditors and the person managing an audit programme should:

— perform their work with honesty, diligence, and responsibility;

— observe and comply with any applicable legal requirements;

— demonstrate their competence while performing their work;

— perform their work in an impartial manner, i.e. remain fair and unbiased in all their dealings;

— be sensitive to any influences that may be exerted on their judgement while carrying out an audit.

b) **Fair presentation:** the obligation to report truthfully and accurately

Audit findings, audit conclusions and audit reports should reflect truthfully and accurately the audit activities. Significant obstacles encountered during the audit and unresolved diverging opinions between the audit team and the auditee should be reported. The communication should be truthful, accurate, objective, timely, clear and complete.

c) **Due professional care:** the application of diligence and judgement in auditing

Auditors should exercise due care in accordance with the importance of the task they perform and the confidence placed in them by the audit client and other interested parties. An important factor in carrying out their work with due professional care is having the ability to make reasoned judgements in all audit situations.

d) **Confidentiality:** security of information

Auditors should exercise discretion in the use and protection of information acquired in the course of their duties. Audit information should not be used inappropriately for personal gain by the auditor or the audit client, or in a manner detrimental to the legitimate interests of the auditee. This concept includes the proper handling of sensitive or confidential information.

e) **Independence:** the basis for the impartiality of the audit and objectivity of the audit conclusions

Auditors should be independent of the activity being audited wherever practicable, and should in all cases act in a manner that is free from bias and conflict of interest. For internal audits, auditors should be independent from the operating managers of the function being audited. Auditors should maintain

objectivity throughout the audit process to ensure that the audit findings and conclusions are based only on the audit evidence.

For small organizations, it may not be possible for internal auditors to be fully independent of the activity being audited, but every effort should be made to remove bias and encourage objectivity.

f) **Evidence-based approach**: the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process

Audit evidence should be verifiable. It will in general be based on samples of the information available, since an audit is conducted during a finite period of time and with finite resources. An appropriate use of sampling should be applied, since this is closely related to the confidence that can be placed in the audit conclusions.

5 Managing an audit programme

5.1 General

An organization needing to conduct audits should establish an audit programme that contributes to the determination of the effectiveness of the auditee's management system. The audit programme can include audits considering one or more management system standards, conducted either separately or in combination.

The top management should ensure that the audit programme objectives are established and assign one or more competent persons to manage the audit programme. The extent of an audit programme should be based on the size and nature of the organization being audited, as well as on the nature, functionality, complexity and the level of maturity of the management system to be audited. Priority should be given to allocating the audit programme resources to audit those matters of significance within the management system. These may include the key characteristics of product quality or hazards related to health and safety, or significant environmental aspects and their control.

NOTE This concept is commonly known as risk-based auditing. This International Standard does not give further guidance on risk-based auditing.

The audit programme should include information and resources necessary to organize and conduct its audits effectively and efficiently within the specified time frames and can also include the following:

— objectives for the audit programme and individual audits;

— extent/number/types/duration/locations/schedule of the audits;

— audit programme procedures;

— audit criteria;

— audit methods;

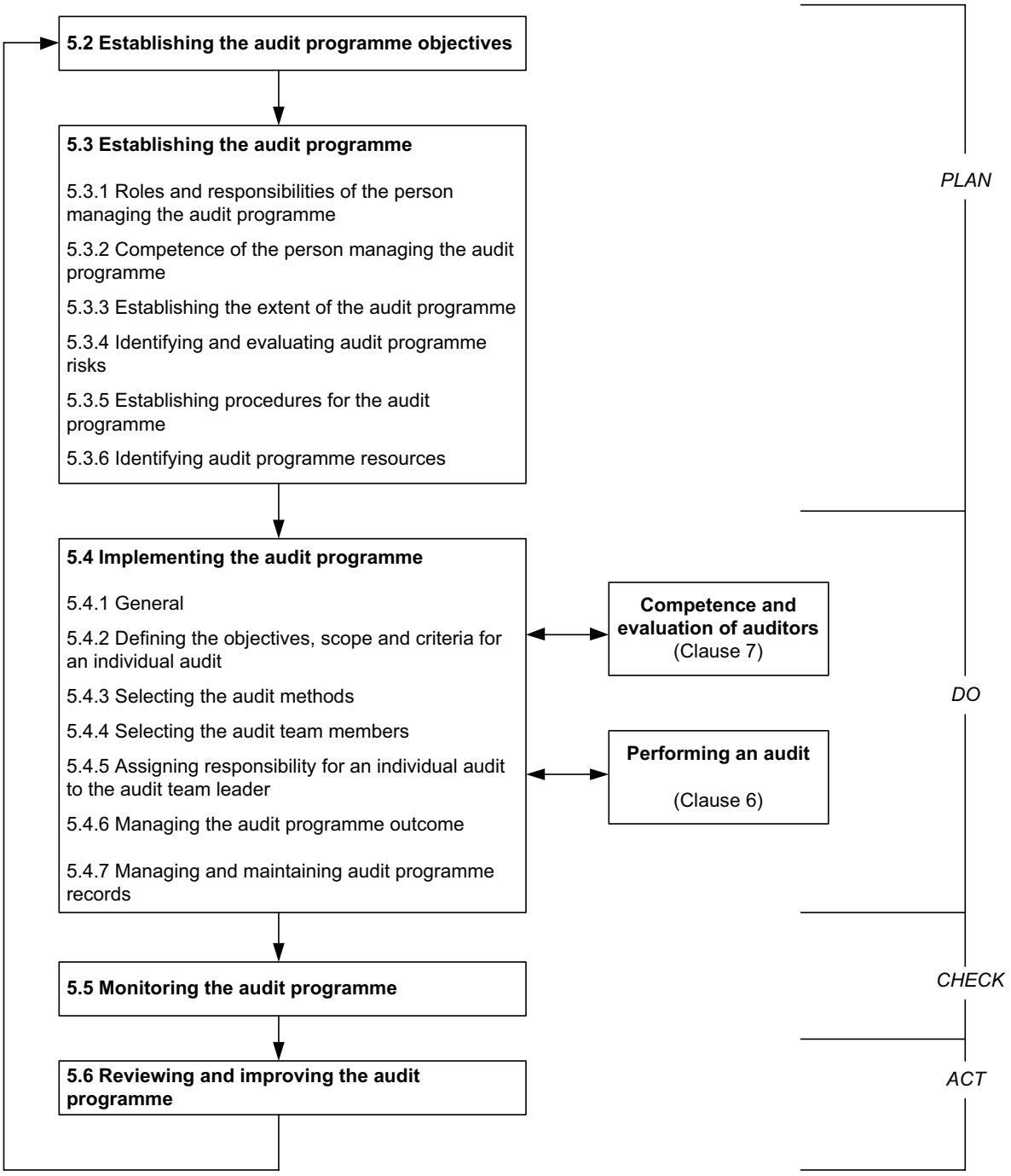
— selection of audit teams;

— necessary resources, including travel and accommodation;

— processes for handling confidentiality, information security, health and safety, and other similar matters.

The implementation of the audit programme should be monitored and measured to ensure its objectives have been achieved. The audit programme should be reviewed in order to identify possible improvements.

Figure 1 illustrates the process flow for the management of an audit programme.



NOTE 1 This figure illustrates the application of the Plan-Do-Check-Act cycle in this International Standard.

NOTE 2 Clause/subclause numbering refers to the relevant clauses/subclauses of this International Standard.

Figure 1 — Process flow for the management of an audit programme

5.2 Establishing the audit programme objectives

The top management should ensure that the audit programme objectives are established to direct the planning and conduct of audits and should ensure the audit programme is implemented effectively. Audit programme objectives should be consistent with and support management system policy and objectives.

These objectives can be based on consideration of the following:

a) management priorities;

b) commercial and other business intentions;

c) characteristics of processes, products and projects, and any changes to them;

d) management system requirements;

e) legal and contractual requirements and other requirements to which the organization is committed;

f) need for supplier evaluation;

g) needs and expectations of interested parties, including customers;

h) auditee's level of performance, as reflected in the occurrence of failures or incidents or customer complaints;

i) risks to the auditee;

j) results of previous audits;

k) level of maturity of the management system being audited.

Examples of audit programme objectives include the following:

— to contribute to the improvement of a management system and its performance;

— to fulfil external requirements, e.g. certification to a management system standard;

— to verify conformity with contractual requirements;

— to obtain and maintain confidence in the capability of a supplier;

— to determine the effectiveness of the management system;

— to evaluate the compatibility and alignment of the management system objectives with the management system policy and the overall organizational objectives.

5.3 Establishing the audit programme

5.3.1 Roles and responsibilities of the person managing the audit programme

The person managing the audit programme should:

— establish the extent of the audit programme;

— identify and evaluate the risks for the audit programme;

— establish audit responsibilities;

— establish procedures for audit programmes;

— determine necessary resources;

— ensure the implementation of the audit programme, including the establishment of audit objectives, scope and criteria of the individual audits, determining audit methods and selecting the audit team and evaluating auditors;

— ensure that appropriate audit programme records are managed and maintained;

— monitor, review and improve the audit programme.

The person managing an audit programme should inform the top management of the contents of the audit programme and, where necessary, request its approval.

5.3.2 Competence of the person managing the audit programme

The person managing the audit programme should have the necessary competence to manage the programme and its associated risks effectively and efficiently, as well as knowledge and skills in the following areas:

— audit principles, procedures and methods;

— management system standards and reference documents;

— activities, products and processes of the auditee;

— applicable legal and other requirements relevant to the activities and products of the auditee;

— customers, suppliers and other interested parties of the auditee, where applicable.

The person managing the audit programme should engage in appropriate continual professional development activities to maintain the necessary knowledge and skills to manage the audit programme.

5.3.3 Establishing the extent of the audit programme

The person managing the audit programme should determine the extent of the audit programme, which can vary depending on the size and nature of the auditee, as well as on the nature, functionality, complexity and the level of maturity of, and matters of significance to, the management system to be audited.

NOTE In certain cases, depending on the auditee's structure or its activities, the audit programme might only consist of a single audit (e.g. a small project activity).

Other factors impacting the extent of an audit programme include the following:

— the objective, scope and duration of each audit and the number of audits to be conducted, including audit follow up, if applicable;

— the number, importance, complexity, similarity and locations of the activities to be audited;

— those factors influencing the effectiveness of the management system;

— applicable audit criteria, such as planned arrangements for the relevant management standards, legal and contractual requirements and other requirements to which the organization is committed;

— conclusions of previous internal or external audits;

— results of a previous audit programme review;

— language, cultural and social issues;

— the concerns of interested parties, such as customer complaints or non-compliance with legal requirements;

— significant changes to the auditee or its operations;

— availability of information and communication technologies to support audit activities, in particular the use of remote audit methods (see Clause B.1);

— the occurrence of internal and external events, such as product failures, information security leaks, health and safety incidents, criminal acts or environmental incidents.

5.3.4 Identifying and evaluating audit programme risks

There are many different risks associated with establishing, implementing, monitoring, reviewing and improving an audit programme that may affect the achievement of its objectives. The person managing the programme should consider these risks in its development. These risks may be associated with the following:

— planning, e.g. failure to set relevant audit objectives and determine the extent of the audit programme;

— resources, e.g. allowing insufficient time for developing the audit programme or conducting an audit;

— selection of the audit team, e.g. the team does not have the collective competence to conduct audits effectively;

— implementation, e.g. ineffective communication of the audit programme;

— records and their controls, e.g. failure to adequately protect audit records to demonstrate audit programme effectiveness;

— monitoring, reviewing and improving the audit programme, e.g. ineffective monitoring of audit programme outcomes.

5.3.5 Establishing procedures for the audit programme

The person managing the audit programme should establish one or more procedures, addressing the following, as applicable:

— planning and scheduling audits considering audit programme risks;

— ensuring information security and confidentiality;

— assuring the competence of auditors and audit team leaders;

— selecting appropriate audit teams and assigning their roles and responsibilities;

— conducting audits, including the use of appropriate sampling methods;

— conducting audit follow-up, if applicable;

— reporting to the top management on the overall achievements of the audit programme;

— maintaining audit programme records;

— monitoring and reviewing the performance and risks, and improving the effectiveness of the audit programme.

5.3.6 Identifying audit programme resources

When identifying resources for the audit programme, the person managing the audit programme should consider:

— the financial resources necessary to develop, implement, manage and improve audit activities;

— audit methods;

— the availability of auditors and technical experts having competence appropriate to the particular audit programme objectives;

— the extent of the audit programme and audit programme risks;

— travelling time and cost, accommodation and other auditing needs;

— the availability of information and communication technologies.

5.4 Implementing the audit programme

5.4.1 General

The person managing the audit programme should implement the audit programme by means of the following:

— communicating the pertinent parts of the audit programme to relevant parties and informing them periodically of its progress;

— defining objectives, scope and criteria for each individual audit;

— coordinating and scheduling audits and other activities relevant to the audit programme;

— ensuring the selection of audit teams with the necessary competence;

— providing necessary resources to the audit teams;

— ensuring the conduct of audits in accordance with the audit programme and within the agreed time frame;

— ensuring that audit activities are recorded and records are properly managed and maintained.

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

Each individual audit should be based on documented audit objectives, scope and criteria. These should be defined by the person managing the audit programme and be consistent with the overall audit programme objectives.

The audit objectives define what is to be accomplished by the individual audit and may include the following:

— determination of the extent of conformity of the management system to be audited, or parts of it, with audit criteria;

— determination of the extent of conformity of activities, processes and products with the requirements and procedures of the management system;

— evaluation of the capability of the management system to ensure compliance with legal and contractual requirements and other requirements to which the organization is committed;

— evaluation of the effectiveness of the management system in meeting its specified objectives;

— identification of areas for potential improvement of the management system.

The audit scope should be consistent with the audit programme and audit objectives. It includes such factors as physical locations, organizational units, activities and processes to be audited, as well as the time period covered by the audit.

The audit criteria are used as a reference against which conformity is determined and may include applicable policies, procedures, standards, legal requirements, management system requirements, contractual requirements, sector codes of conduct or other planned arrangements.

In the event of any changes to the audit objectives, scope or criteria, the audit programme should be modified if necessary.

When two or more management systems of different disciplines are audited together (a combined audit), it is important that the audit objectives, scope and criteria are consistent with the objectives of the relevant audit programmes.

5.4.3 Selecting the audit methods

The person managing the audit programme should select and determine the methods for effectively conducting an audit, depending on the defined audit objectives, scope and criteria.

NOTE Guidance on how to determine audit methods is given in Annex B.

Where two or more auditing organizations conduct a joint audit of the same auditee, the persons managing the different audit programmes should agree on the audit method and consider implications for resourcing and planning the audit. If an auditee operates two or more management systems of different disciplines, combined audits may be included in the audit programme.

5.4.4 Selecting the audit team members

The person managing the audit programme should appoint the members of the audit team, including the team leader and any technical experts needed for the specific audit.

An audit team should be selected, taking into account the competence needed to achieve the objectives of the individual audit within the defined scope. If there is only one auditor, the auditor should perform all applicable duties of an audit team leader.

NOTE Clause 7 contains guidance on determining the competence required for the audit team members and describes the processes for evaluating auditors.

In deciding the size and composition of the audit team for the specific audit, consideration should be given to the following:

a) the overall competence of the audit team needed to achieve audit objectives, taking into account audit scope and criteria;

b) complexity of the audit and if the audit is a combined or joint audit;

c) the audit methods that have been selected;

d) legal and contractual requirements and other requirements to which the organization is committed;

e) the need to ensure the independence of the audit team members from the activities to be audited and to avoid any conflict of interest [see principle e) in Clause 4];

f) the ability of the audit team members to interact effectively with the representatives of the auditee and to work together;

g) the language of the audit, and the auditee's social and cultural characteristics. These issues may be addressed either by the auditor's own skills or through the support of a technical expert.

To assure the overall competence of the audit team, the following steps should be performed:

— identification of the knowledge and skills needed to achieve the objectives of the audit;

— selection of the audit team members so that all of the necessary knowledge and skills are present in the audit team.

If all the necessary competence is not covered by the auditors in the audit team, technical experts with additional competence should be included in the team. Technical experts should operate under the direction of an auditor, but should not act as auditors.

Auditors-in-training may be included in the audit team, but should participate under the direction and guidance of an auditor.

Adjustments to the size and composition of the audit team may be necessary during the audit, i.e. if a conflict of interest or competence issue arises. If such a situation arises, it should be discussed with the appropriate parties (e.g. audit team leader, the person managing the audit programme, audit client or auditee) before any adjustments are made.

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

The person managing the audit programme should assign the responsibility for conducting the individual audit to an audit team leader.

The assignment should be made in sufficient time before the scheduled date of the audit, in order to ensure the effective planning of the audit.

To ensure effective conduct of the individual audits, the following information should be provided to the audit team leader:

a) audit objectives;

b) audit criteria and any reference documents;

c) audit scope, including identification of the organizational and functional units and processes to be audited;

d) audit methods and procedures;

e) composition of the audit team;

f) contact details of the auditee, the locations, dates and duration of the audit activities to be conducted;

g) allocation of appropriate resources to conduct the audit;

h) information needed for evaluating and addressing identified risks to the achievement of the audit objectives.

The assignment information should also cover the following, as appropriate:

— working and reporting language of the audit where this is different from the language of the auditor or the auditee, or both;

— audit report contents and distribution required by the audit programme;

— matters related to confidentiality and information security, if required by the audit programme;

— any health and safety requirements for the auditors;

— any security and authorization requirements;

— any follow-up actions, e.g. from a previous audit, if applicable;

— coordination with other audit activities, in the case of a joint audit.

Where a joint audit is conducted, it is important to reach agreement among the organizations conducting the audits, before the audit commences, on the specific responsibilities of each party, particularly with regard to the authority of the team leader appointed for the audit.

5.4.6 Managing the audit programme outcome

The person managing the audit programme should ensure that the following activities are performed:

— review and approval of audit reports, including evaluating the suitability and adequacy of audit findings;

— review of root cause analysis and the effectiveness of corrective actions and preventive actions;

— distribution of audit reports to the top management and other relevant parties;

— determination of the necessity for any follow-up audit.

5.4.7 Managing and maintaining audit programme records

The person managing the audit programme should ensure that audit records are created, managed and maintained to demonstrate the implementation of the audit programme. Processes should be established to ensure that any confidentiality needs associated with the audit records are addressed.

Records should include the following:

a) records related to the audit programme, such as:

   — documented audit programme objectives and extent;

   — those addressing audit programme risks;

   — reviews of the audit programme effectiveness;

b) records related to each individual audit, such as:

   — audit plans and audit reports;

   — nonconformity reports;

   — corrective and preventive action reports;

   — audit follow-up reports, if applicable;

c) records related to audit personnel covering topics such as:

   — competence and performance evaluation of the audit team members;

   — selection of audit teams and team members;

   — maintenance and improvement of competence.

The form and level of detail of the records should demonstrate that the objectives of the audit programme have been achieved.

5.5 Monitoring the audit programme

The person managing the audit programme should monitor its implementation considering the need to:

a) evaluate conformity with audit programmes, schedules and audit objectives;

b) evaluate the performance of the audit team members;

c) evaluate the ability of the audit teams to implement the audit plan;

d) evaluate feedback from top management, auditees, auditors and other interested parties.

Some factors may determine the need to modify the audit programme, such as the following:

— audit findings;

— demonstrated level of management system effectiveness;

— changes to the client's or the auditee's management system;

— changes to standards, legal and contractual requirements and other requirements to which the organization is committed;

— change of supplier.

5.6 Reviewing and improving the audit programme

The person managing the audit programme should review the audit programme to assess whether its objectives have been achieved. Lessons learned from the audit programme review should be used as inputs for the continual improvement process for the programme.

The audit programme review should consider the following:

a) results and trends from audit programme monitoring;

b) conformity with audit programme procedures;

c) evolving needs and expectations of interested parties;

d) audit programme records;

e) alternative or new auditing methods;

f) effectiveness of the measures to address the risks associated with the audit programme;

g) confidentiality and information security issues relating to the audit programme.

The person managing the audit programme should review the overall implementation of the audit programme, identify areas of improvement, amend the programme if necessary, and should also:

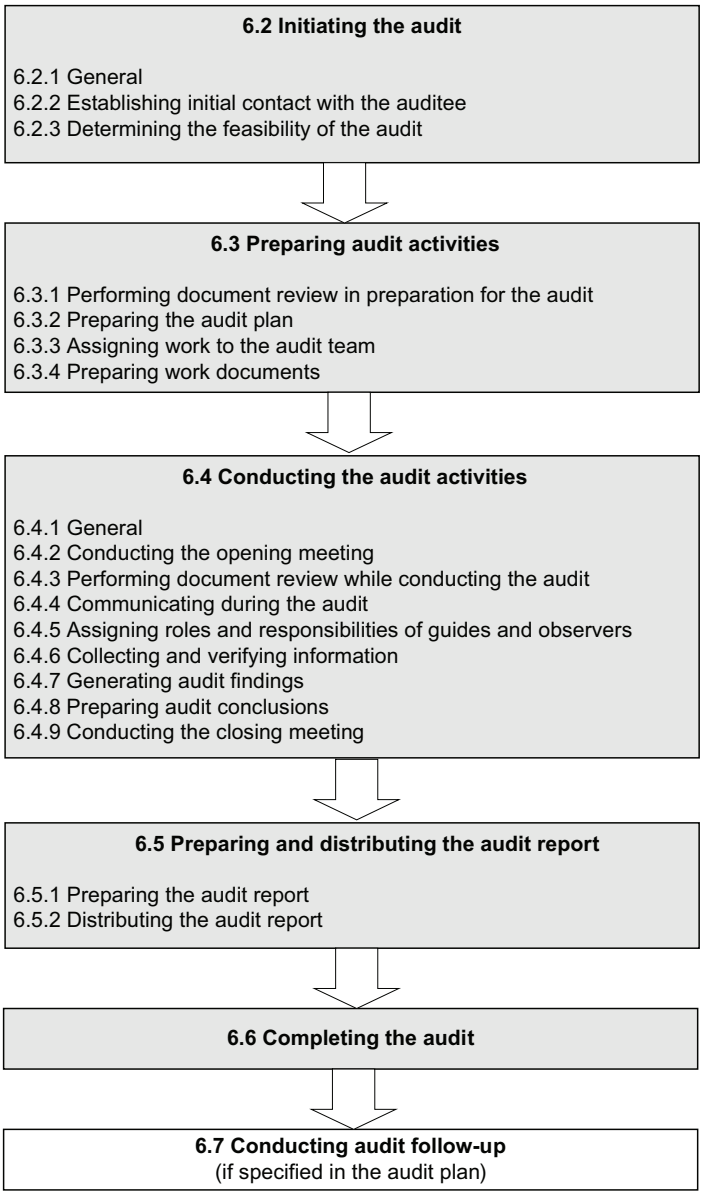
— review the continual professional development of auditors, in accordance with 7.4, 7.5 and 7.6;

— report the results of the audit programme review to the top management.

6 Performing an audit

6.1 General

This clause contains guidance on preparing and conducting audit activities as part of an audit programme. Figure 2 provides an overview of typical audit activities. The extent to which the provisions of this clause are applicable depends on the objectives and scope of the specific audit.



NOTE Subclause numbering refers to the relevant subclauses of this International Standard.

Figure 2 — Typical audit activities

6.2 Initiating the audit

6.2.1 General

When an audit is initiated, the responsibility for conducting the audit remains with the assigned audit team leader (see 5.4.5) until the audit is completed (see 6.6).

To initiate an audit, the steps in Figure 2 should be considered; however, the sequence can differ depending on the auditee, processes and specific circumstances of the audit.

6.2.2 Establishing initial contact with the auditee

The initial contact with the auditee for the performance of the audit can be informal or formal and should be made by the audit team leader. The purposes of the initial contact are the following:

— establish communications with the auditee's representatives;

— confirm the authority to conduct the audit;

— provide information on the audit objectives, scope, methods and audit team composition, including technical experts;

— request access to relevant documents and records for planning purposes;

— determine applicable legal and contractual requirements and other requirements relevant to the activities and products of the auditee;

— confirm the agreement with the auditee regarding the extent of the disclosure and the treatment of confidential information;

— make arrangements for the audit including scheduling the dates;

— determine any location-specific requirements for access, security, health and safety or other;

— agree on the attendance of observers and the need for guides for the audit team;

— determine any areas of interest or concern to the auditee in relation to the specific audit.

6.2.3 Determining the feasibility of the audit

The feasibility of the audit should be determined to provide reasonable confidence that the audit objectives can be achieved.

The determination of feasibility should take into consideration such factors as the availability of the following:

— sufficient and appropriate information for planning and conducting the audit;

— adequate cooperation from the auditee;

— adequate time and resources for conducting the audit.

Where the audit is not feasible, an alternative should be proposed to the audit client, in agreement with the auditee.

6.3 Preparing audit activities

6.3.1 Performing document review in preparation for the audit

The relevant management system documentation of the auditee should be reviewed in order to:

— gather information to prepare audit activities and applicable work documents (see 6.3.4), e.g. on processes, functions;

— establish an overview of the extent of the system documentation to detect possible gaps.

NOTE Guidance on how to perform a document review is provided in Clause B.2.

The documentation should include, as applicable, management system documents and records, as well as previous audit reports. The document review should take into account the size, nature and complexity of the auditee's management system and organization, and the audit objectives and scope.

6.3.2 Preparing the audit plan

6.3.2.1 The audit team leader should prepare an audit plan based on the information contained in the audit programme and in the documentation provided by the auditee. The audit plan should consider the effect of the audit activities on the auditee's processes and provide the basis for the agreement among the audit client, audit team and the auditee regarding the conduct of the audit. The plan should facilitate the efficient scheduling and coordination of the audit activities in order to achieve the objectives effectively.

The amount of detail provided in the audit plan should reflect the scope and complexity of the audit, as well as the effect of uncertainty on achieving the audit objectives. In preparing the audit plan, the audit team leader should be aware of the following:

— the appropriate sampling techniques (see Clause B.3);

— the composition of the audit team and its collective competence;

— the risks to the organization created by the audit.

For example, risks to the organization may result from the presence of the audit team members influencing health and safety, environment and quality, and their presence presenting threats to the auditee's products, services, personnel or infrastructure (e.g. contamination in clean room facilities).

For combined audits, particular attention should be given to the interactions between operational processes and the competing objectives and priorities of the different management systems.

6.3.2.2 The scale and content of the audit plan may differ, for example, between initial and subsequent audits, as well as between internal and external audits. The audit plan should be sufficiently flexible to permit changes which can become necessary as the audit activities progress.

The audit plan should cover or reference the following:

a) the audit objectives;

b) the audit scope, including identification of the organizational and functional units, as well as processes to be audited;

c) the audit criteria and any reference documents;

d) the locations, dates, expected time and duration of audit activities to be conducted, including meetings with the auditee's management;

e) the audit methods to be used, including the extent to which audit sampling is needed to obtain sufficient audit evidence and the design of the sampling plan, if applicable;

f) the roles and responsibilities of the audit team members, as well as guides and observers;

g) the allocation of appropriate resources to critical areas of the audit.

The audit plan may also cover the following, as appropriate:

— identification of the auditee's representative for the audit;

— the working and reporting language of the audit where this is different from the language of the auditor or the auditee or both;

— the audit report topics;

— logistics and communications arrangements, including specific arrangements for the locations to be audited;

— any specific measures to be taken to address the effect of uncertainty on achieving the audit objectives;

— matters related to confidentiality and information security;

— any follow-up actions from a previous audit;

— any follow-up activities to the planned audit;

— coordination with other audit activities, in case of a joint audit.

The audit plan may be reviewed and accepted by the audit client, and should be presented to the auditee. Any objections by the auditee to the audit plan should be resolved between the audit team leader, the auditee and the audit client.

6.3.3 Assigning work to the audit team

The audit team leader, in consultation with the audit team, should assign to each team member responsibility for auditing specific processes, activities, functions or locations. Such assignments should take into account the independence and competence of auditors and the effective use of resources, as well as different roles and responsibilities of auditors, auditors-in-training and technical experts.

Audit team briefings should be held, as appropriate, by the audit team leader in order to allocate work assignments and decide possible changes. Changes to the work assignments can be made as the audit progresses in order to ensure the achievement of the audit objectives.

6.3.4 Preparing work documents

The audit team members should collect and review the information relevant to their audit assignments and prepare work documents, as necessary, for reference and for recording audit evidence. Such work documents may include the following:

— checklists;

— audit sampling plans;

— forms for recording information, such as supporting evidence, audit findings and records of meetings.

The use of checklists and forms should not restrict the extent of audit activities, which can change as a result of information collected during the audit.

NOTE Guidance on preparing work documents is given in Clause B.4.

Work documents, including records resulting from their use, should be retained at least until audit completion, or as specified in the audit plan. Retention of documents after audit completion is described in 6.6. Those documents involving confidential or proprietary information should be suitably safeguarded at all times by the audit team members.

6.4 Conducting the audit activities

6.4.1 General

Audit activities are normally conducted in a defined sequence as indicated in Figure 2. This sequence may be varied to suit the circumstances of specific audits.

6.4.2 Conducting the opening meeting

The purpose of the opening meeting is to:

a) confirm the agreement of all parties (e.g. auditee, audit team) to the audit plan;

b) introduce the audit team;

c) ensure that all planned audit activities can be performed.

An opening meeting should be held with the auditee's management and, where appropriate, those responsible for the functions or processes to be audited. During the meeting, an opportunity to ask questions should be provided.

The degree of detail should be consistent with the familiarity of the auditee with the audit process. In many instances, e.g. internal audits in a small organization, the opening meeting may simply consist of communicating that an audit is being conducted and explaining the nature of the audit.

For other audit situations, the meeting may be formal and records of attendance should be kept. The meeting should be chaired by the audit team leader, and the following items should be considered, as appropriate:

— introduction of the participants, including observers and guides, and an outline of their roles;

— confirmation of the audit objectives, scope and criteria;

— confirmation of the audit plan and other relevant arrangements with the auditee, such as the date and time for the closing meeting, any interim meetings between the audit team and the auditee's management, and any late changes;

— presentation of the methods to be used to conduct the audit, including advising the auditee that the audit evidence will be based on a sample of the information available;

— introduction of the methods to manage risks to the organization which may result from the presence of the audit team members;

— confirmation of formal communication channels between the audit team and the auditee;

— confirmation of the language to be used during the audit;

— confirmation that, during the audit, the auditee will be kept informed of audit progress;

— confirmation that the resources and facilities needed by the audit team are available;

— confirmation of matters relating to confidentiality and information security;

— confirmation of relevant health and safety, emergency and security procedures for the audit team;

— information on the method of reporting audit findings including grading, if any;

— information about conditions under which the audit may be terminated;

— information about the closing meeting;

— information about how to deal with possible findings during the audit;

— information about any system for feedback from the auditee on the findings or conclusions of the audit, including complaints or appeals.

6.4.3 Performing document review while conducting the audit

The auditee's relevant documentation should be reviewed to:

— determine the conformity of the system, as far as documented, with audit criteria;

— gather information to support the audit activities.

NOTE Guidance on how to perform a document review is provided in Clause B.2.

The review may be combined with the other audit activities and may continue throughout the audit, providing this is not detrimental to the effectiveness of the conduct of the audit.

If adequate documentation cannot be provided within the time frame given in the audit plan, the audit team leader should inform both the person managing the audit programme and the auditee. Depending on the audit

objectives and scope, a decision should be made as to whether the audit should be continued or suspended until documentation concerns are resolved.

6.4.4 Communicating during the audit

During the audit, it may be necessary to make formal arrangements for communication within the audit team, as well as with the auditee, the audit client and potentially with external bodies (e.g. regulators), especially where legal requirements require the mandatory reporting of non-compliances.

The audit team should confer periodically to exchange information, assess audit progress, and reassign work between the audit team members, as needed.

During the audit, the audit team leader should periodically communicate the progress of the audit and any concerns to the auditee and audit client, as appropriate. Evidence collected during the audit that suggests an immediate and significant risk to the auditee should be reported without delay to the auditee and, as appropriate, to the audit client. Any concern about an issue outside the audit scope should be noted and reported to the audit team leader, for possible communication to the audit client and auditee.

Where the available audit evidence indicates that the audit objectives are unattainable, the audit team leader should report the reasons to the audit client and the auditee to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit.

Any need for changes to the audit plan which may become apparent as auditing activities progress should be reviewed and approved, as appropriate, by both the person managing the audit programme and the auditee.

6.4.5 Assigning roles and responsibilities of guides and observers

Guides and observers (e.g. regulator or other interested parties) may accompany the audit team. They should not influence or interfere with the conduct of the audit. If this cannot be assured, the audit team leader should have the right to deny observers from taking part in certain audit activities.

For observers, any obligations in relation to health and safety, security and confidentiality should be managed between the audit client and the auditee.

Guides, appointed by the auditee, should assist the audit team and act on the request of the audit team leader. Their responsibilities should include the following:

a) assisting the auditors in identifying individuals to participate in interviews and confirming timings;

b) arranging access to specific locations of the auditee;

c) ensuring that rules concerning location safety and security procedures are known and respected by the audit team members and observers.

The role of the guide may also include the following:

— witnessing the audit on behalf of the auditee;

— providing clarification or assisting in collecting information.

6.4.6 Collecting and verifying information

During the audit, information relevant to the audit objectives, scope and criteria, including information relating to interfaces between functions, activities and processes, should be collected 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. If, during the collection of evidence, the audit team becomes aware of any new or changed circumstances or risks, these should be addressed by the team accordingly.

NOTE 1 Guidance on sampling is given in Clause B.3.

Figure 3 provides an overview of the process, from collecting information to reaching audit conclusions.

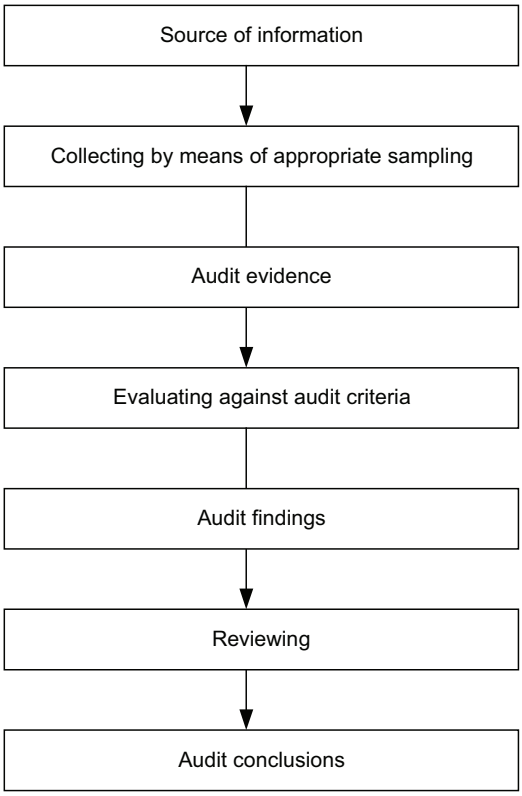


Figure 3 — Overview of the process of collecting and verifying information

Methods of collecting information include the following:

— interviews;

— observations;

— review of documents, including records.

NOTE 2 Guidance on sources of information is given in Clause B.5.

NOTE 3 Guidance on visiting the auditee's location is given in Clause B.6.

NOTE 4 Guidance on how to conduct interviews is given in Clause B.7.

6.4.7 Generating audit findings

Audit evidence should be evaluated against the audit criteria in order to determine audit findings. Audit findings can indicate conformity or nonconformity with audit criteria. When specified by the audit plan, individual audit findings should include conformity and good practices along with their supporting evidence, opportunities for improvement, and any recommendations to the auditee.

Nonconformities and their supporting audit evidence should be recorded. Nonconformities may be graded. They should be reviewed with the auditee in order to obtain acknowledgement that the audit evidence is accurate, and that the nonconformities are understood. Every attempt should be made to resolve any diverging opinions concerning the audit evidence or findings, and unresolved points should be recorded.

The audit team should meet as needed to review the audit findings at appropriate stages during the audit.

NOTE Additional guidance on the identification and evaluation of audit findings is given in Clause B.8.

6.4.8 Preparing audit conclusions

The audit team should confer prior to the closing meeting in order to:

a) review the audit findings, and any other appropriate information collected during the audit, against the audit objectives;

b) agree on the audit conclusions, taking into account the uncertainty inherent in the audit process;

c) prepare recommendations, if specified by the audit plan;

d) discuss audit follow-up, as applicable.

Audit conclusions can address issues such as the following:

— the extent of conformity with the audit criteria and robustness of the management system, including the effectiveness of the management system in meeting the stated objectives;

— the effective implementation, maintenance and improvement of the management system;

— the capability of the management review process to ensure the continuing suitability, adequacy, effectiveness and improvement of the management system;

— achievement of audit objectives, coverage of audit scope, and fulfilment of audit criteria;

— root causes of findings, if included in the audit plan;

— similar findings made in different areas that were audited for the purpose of identifying trends.

If specified by the audit plan, audit conclusions can lead to recommendations for improvement, or future auditing activities.

6.4.9 Conducting the closing meeting

A closing meeting, facilitated by the audit team leader, should be held to present the audit findings and conclusions. Participants in the closing meeting should include the management of the auditee and, where appropriate, those responsible for the functions or processes which have been audited, and may also include the audit client and other parties. If applicable, the audit team leader should advise the auditee of situations encountered during the audit that may decrease the confidence that can be placed in the audit conclusions. If defined in the management system or by agreement with the audit client, the participants should agree on the time frame for an action plan to address audit findings.

The degree of detail should be consistent with the familiarity of the auditee with the audit process. For some audit situations, the meeting may be formal and minutes, including records of attendance, should be kept. In other instances, e.g. internal audits, the closing meeting is less formal and may consist solely of communicating the audit findings and audit conclusions.

As appropriate, the following should be explained to the auditee in the closing meeting:

— advising that the audit evidence collected was based on a sample of the information available;

— the method of reporting;

— the process of handling of audit findings and possible consequences;

— presentation of the audit findings and conclusions in such a manner that they are understood and acknowledged by the auditee's management;

— any related post-audit activities (e.g. implementation of corrective actions, audit complaint handling, appeal process).

Any diverging opinions regarding the audit findings or conclusions between the audit team and the auditee should be discussed and, if possible, resolved. If not resolved, this should be recorded.

If specified by the audit objectives, recommendations for improvements may be presented. It should be emphasized that recommendations are not binding.

6.5 Preparing and distributing the audit report

6.5.1 Preparing the audit report

The audit team leader should report the audit results in accordance with the audit programme procedures.

The audit report should provide a complete, accurate, concise and clear record of the audit, and should include or refer to the following:

a) the audit objectives;

b) the audit scope, particularly identification of the organizational and functional units or processes audited;

c) identification of the audit client;

d) identification of audit team and auditee's participants in the audit;

e) the dates and locations where the audit activities were conducted;

f) the audit criteria;

g) the audit findings and related evidence;

h) the audit conclusions;

i) a statement on the degree to which the audit criteria have been fulfilled.

The audit report can also include or refer to the following, as appropriate:

— the audit plan including time schedule;

— a summary of the audit process, including any obstacles encountered that may decrease the reliability of the audit conclusions;

— confirmation that the audit objectives have been achieved within the audit scope in accordance with the audit plan;

— any areas within the audit scope not covered;

— a summary covering the audit conclusions and the main audit findings that support them;

— any unresolved diverging opinions between the audit team and the auditee;

— opportunities for improvement, if specified in the audit plan;

— good practices identified;

— agreed follow-up action plans, if any;

— a statement of the confidential nature of the contents;

— any implications for the audit programme or subsequent audits;

— the distribution list for the audit report.

NOTE The audit report can be developed before the closing meeting.

6.5.2 Distributing the audit report

The audit report should be issued within an agreed period of time. If it is delayed, the reasons should be communicated to the auditee and the person managing the audit programme.

The audit report should be dated, reviewed and approved, as appropriate, in accordance with audit programme procedures.

The audit report should then be distributed to the recipients as defined in the audit procedures or audit plan.

6.6 Completing the audit

The audit is completed when all planned audit activities have been carried out, or as otherwise agreed with the audit client (e.g. there might be an unexpected situation that prevents the audit being completed according to the plan).

Documents pertaining to the audit should be retained or destroyed by agreement between the participating parties and in accordance with audit programme procedures and applicable requirements.

Unless required by law, the audit team and the person managing the audit programme should not disclose the contents of documents, any other information obtained during the audit, or the audit report, to any other party without the explicit approval of the audit client and, where appropriate, the approval of the auditee. If disclosure of the contents of an audit document is required, the audit client and auditee should be informed as soon as possible.

Lessons learned from the audit should be entered into the continual improvement process of the management system of the audited organizations.

6.7 Conducting audit follow-up

The conclusions of the audit can, depending on the audit objectives, indicate the need for corrections, or for corrective, preventive or improvement actions. Such actions are usually decided and undertaken by the auditee within an agreed timeframe. As appropriate, the auditee should keep the person managing the audit programme and the audit team informed of the status of these actions.

The completion and effectiveness of these actions should be verified. This verification may be part of a subsequent audit.

7 Competence and evaluation of auditors

7.1 General

Confidence in the audit process and the ability to achieve its objectives depends on the competence of those individuals who are involved in planning and conducting audits, including auditors and audit team leaders. Competence should be evaluated through a process that considers personal behaviour and the ability to apply the knowledge and skills gained through education, work experience, auditor training and audit experience. This process should take into consideration the needs of the audit programme and its objectives. Some of the knowledge and skills described in 7.2.3 are common to auditors of any management system discipline; others are specific to individual management system disciplines. It is not necessary for each auditor in the audit team to have the same competence; however, the overall competence of the audit team needs to be sufficient to achieve the audit objectives.

The evaluation of auditor competence should be planned, implemented and documented in accordance with the audit programme, including its procedures to provide an outcome that is objective, consistent, fair and reliable. The evaluation process should include four main steps, as follows:

a) determine the competence of audit personnel to fulfil the needs of the audit programme;

b) establish the evaluation criteria;

c) select the appropriate evaluation method;

d) conduct the evaluation.

The outcome of the evaluation process should provide a basis for the following:

— selection of audit team members as described in 5.4.4;

— determining the need for improved competence (e.g. additional training);

— ongoing performance evaluation of auditors.

Auditors should develop, maintain and improve their competence through continual professional development and regular participation in audits (see 7.6).

A process for evaluating auditors and audit team leaders is described in 7.4 and 7.5.

Auditors and audit team leaders should be evaluated against the criteria set out in 7.2.2 and 7.2.3.

The competence required of the person managing the audit programme is described in 5.3.2.

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

7.2.1 General

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

— the size, nature and complexity of the organization to be audited;

— the management system disciplines to be audited;

— the objectives and extent of the audit programme;

— other requirements, such as those imposed by external bodies, where appropriate;

— the role of the audit process in the management system of the auditee;

— the complexity of the management system to be audited;

— the uncertainty in achieving audit objectives.

This information should be matched against that listed in 7.2.3.2, 7.2.3.3 and 7.2.3.4.

7.2.2 Personal behaviour

Auditors should possess the necessary qualities to enable them to act in accordance with the principles of auditing as described in Clause 4. Auditors should exhibit professional behaviour during the performance of audit activities, including being:

— ethical, i.e. fair, truthful, sincere, honest and discreet;

— open-minded, i.e. willing to consider alternative ideas or points of view;

— diplomatic, i.e. tactful in dealing with people;

— observant, i.e. actively observing physical surroundings and activities;

— perceptive, i.e. aware of and able to understand situations;

— versatile, i.e. able to readily adapt to different situations;

— tenacious, i.e. persistent and focused on achieving objectives;

— decisive, i.e. able to reach timely conclusions based on logical reasoning and analysis;

— self-reliant, i.e. able to act and function independently whilst interacting effectively with others;

— acting with fortitude, i.e. able to act responsibly and ethically, even though these actions may not always be popular and may sometimes result in disagreement or confrontation;

— open to improvement, i.e. willing to learn from situations, and striving for better audit results;

— culturally sensitive, i.e. observant and respectful to the culture of the auditee;

— collaborative, i.e. effectively interacting with others, including audit team members and the auditee's personnel.

7.2.3 Knowledge and skills

7.2.3.1 General

Auditors should possess the knowledge and skills necessary to achieve the intended results of the audits they are expected to perform. All auditors should possess generic knowledge and skills and should also be expected to possess some discipline and sector-specific knowledge and skills. Audit team leaders should have the additional knowledge and skills necessary to provide leadership to the audit team.

7.2.3.2 Generic knowledge and skills of management system auditors

Auditors should have knowledge and skills in the areas outlined below.

a) **Audit principles, procedures and methods**: knowledge and skills in this area enable the auditor to apply the appropriate principles, procedures and methods to different audits, and to ensure that audits are conducted in a consistent and systematic manner. An auditor should be able to do the following:

   — apply audit principles, procedures, and methods;

   — plan and organize the work effectively;

   — conduct the audit within the agreed time schedule;

   — prioritize and focus on matters of significance;

   — collect information through effective interviewing, listening, observing and reviewing documents, records and data;

   — understand and consider the experts' opinions;

   — understand the appropriateness and consequences of using sampling techniques for auditing;

   — verify the relevance and accuracy of collected information;

   — confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;

   — assess those factors that may affect the reliability of the audit findings and conclusions;

   — use work documents to record audit activities;

   — document audit findings and prepare appropriate audit reports;

   — maintain the confidentiality and security of information, data, documents and records;

   — communicate effectively, orally and in writing (either personally, or through the use of interpreters and translators);

   — understand the types of risks associated with auditing.

b) **Management system and reference documents**: knowledge and skills in this area enable the auditor to comprehend the audit scope and apply audit criteria, and should cover the following:

   — management system standards or other documents used as audit criteria;

— the application of management system standards by the auditee and other organizations, as appropriate;

— interaction between the components of the management system;

— recognizing the hierarchy of reference documents;

— application of the reference documents to different audit situations.

c) **Organizational context**: knowledge and skills in this area enable the auditor to comprehend the auditee's structure, business and management practices, and should cover the following:

— organizational types, governance, size, structure, functions and relationships;

— general business and management concepts, processes and related terminology, including planning, budgeting and management of personnel;

— cultural and social aspects of the auditee.

d) **Applicable legal and contractual requirements and other requirements that apply to the auditee**: knowledge and skills in this area enable the auditor to be aware of, and work within, the organization's legal and contractual requirements. Knowledge and skills specific to the jurisdiction or to the auditee's activities and products should cover the following:

— laws and regulations and their governing agencies;

— basic legal terminology;

— contracting and liability.

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

Auditors should have the discipline and sector-specific knowledge and skills that are appropriate for auditing the particular type of management system and sector.

It is not necessary for each auditor in the audit team to have the same competence; however, the overall competence of the audit team needs to be sufficient to achieve the audit objectives.

The discipline and sector-specific knowledge and skills of auditors include the following:

— discipline-specific management system requirements and principles, and their application;

— legal requirements relevant to the discipline and sector, such that the auditor is aware of the requirements specific to the jurisdiction and the auditee's obligations, activities and products;

— requirements of interested parties relevant to the specific discipline;

— fundamentals of the discipline and the application of business and technical discipline-specific methods, techniques, processes and practices, sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions;

— discipline-specific knowledge related to the particular sector, nature of operations or workplace being audited, sufficient for the auditor to evaluate the auditee's activities, processes, and products (goods and services);

— risk management principles, methods and techniques relevant to the discipline and sector, such that the auditor can evaluate and control the risks associated with the audit programme.

NOTE Guidance and illustrative examples of discipline-specific knowledge and skills of auditors are provided in Annex A.

7.2.3.4 Generic knowledge and skills of an audit team leader

Audit team leaders should have additional knowledge and skills to manage and provide leadership to the audit team, in order to facilitate the efficient and effective conduct of the audit. An audit team leader should have the knowledge and skills necessary to do the following:

a) balance the strengths and weaknesses of the individual audit team members;

b) develop a harmonious working relationship among the audit team members;

c) manage the audit process, including:

   — planning the audit and making effective use of resources during the audit;

   — managing the uncertainty of achieving audit objectives;

   — protecting the health and safety of the audit team members during the audit, including ensuring compliance of the auditors with the relevant health, safety and security requirements;

   — organizing and directing the audit team members;

   — providing direction and guidance to auditors-in-training;

   — preventing and resolving conflicts, as necessary;

d) represent the audit team in communications with the person managing the audit programme, audit client and auditee;

e) lead the audit team to reach the audit conclusions;

f) prepare and complete the audit report.

7.2.3.5 Knowledge and skills for auditing management systems addressing multiple disciplines

Auditors who intend to participate as an audit team member in auditing management systems addressing multiple disciplines should have the competence necessary to audit at least one of the management system disciplines and an understanding of the interaction and synergy between the different management systems.

Audit team leaders conducting audits of management systems addressing multiple disciplines should understand the requirements of each of the management system standards and recognize the limits of their knowledge and skills in each of the disciplines.

7.2.4 Achieving auditor competence

Auditor knowledge and skills can be acquired using a combination of the following:

— formal education/training and experience that contribute to the development of knowledge and skills in the management system discipline and sector the auditor intends to audit;

— training programmes that cover generic auditor knowledge and skills;

— experience in a relevant technical, managerial or professional position involving the exercise of judgement, decision making, problem solving and communication with managers, professionals, peers, customers and other interested parties;

— audit experience acquired under the supervision of an auditor in the same discipline.

7.2.5 Audit team leaders

An audit team leader should have acquired additional audit experience to develop the knowledge and skills described in 7.2.3. This additional experience should have been gained by working under the direction and guidance of a different audit team leader.

7.3 Establishing the auditor evaluation criteria

The criteria should be qualitative (such as having demonstrated personal behaviour, knowledge or the performance of the skills, in training or in the workplace) and quantitative (such as the years of work experience and education, number of audits conducted, hours of audit training).

7.4 Selecting the appropriate auditor evaluation method

The evaluation should be conducted using two or more of the methods selected from those in Table 2. In using Table 2, the following should be noted:

— the methods outlined represent a range of options and may not apply in all situations;

— the various methods outlined may differ in their reliability;

— a combination of methods should be used to ensure an outcome that is objective, consistent, fair and reliable.

Table 2 — Possible evaluation methods

Evaluation method	Objectives	Examples
Review of records	To verify the background of the auditor	Analysis of records of education, training, employment, professional credentials and audit experience
Feedback	To provide information about how the performance of the auditor is perceived	Surveys, questionnaires, personal references, testimonials, complaints, performance evaluation, peer review
Interview	To evaluate personal behaviour and communication skills, to verify information and test knowledge and to acquire additional information	Personal interviews
Observation	To evaluate personal behaviour and the ability to apply knowledge and skills	Role playing, witnessed audits, on-the-job performance
Testing	To evaluate personal behaviour and knowledge and skills and their application	Oral and written exams, psychometric testing
Post-audit review	To provide information on the auditor performance during the audit activities, identify strengths and weaknesses	Review of the audit report, interviews with the audit team leader, the audit team and, if appropriate, feedback from the auditee.

7.5 Conducting auditor evaluation

The information collected about the person should be compared against the criteria set in 7.2.3. When a person expected to participate in the audit programme does not fulfil the criteria, then additional training, work or audit experience should be undertaken and a subsequent re-evaluation should be performed.

7.6 Maintaining and improving auditor competence

Auditors and audit team leaders should continually improve their competence. Auditors should maintain their auditing competence through regular participation in management system audits and continual professional development. Continual professional development involves the maintenance and improvement of competence. This may be achieved through means such as additional work experience, training, private study, coaching, attendance at meetings, seminars and conferences or other relevant activities.

The person managing the audit programme should establish suitable mechanisms for the continual evaluation of the performance of the auditors, and audit team leaders.

The continual professional development activities should take into account the following:

— changes in the needs of the individual and the organization responsible for the conduct of the audit;

— the practice of auditing;

— relevant standards and other requirements.

Annex A
(informative)

Guidance and illustrative examples of discipline-specific knowledge and skills of auditors

A.1 General

This annex provides generic examples of discipline-specific knowledge and skills for auditors of management systems, which are intended as guidance to assist the person managing the audit programme to select or evaluate auditors.

Other examples of discipline-specific knowledge and skills for auditors may also be developed for management systems. It is suggested that, where possible, such examples follow the same general structure in order to ensure comparability.

A.2 Illustrative example of discipline-specific knowledge and skills of auditors in transportation safety management

Knowledge and skills related to transportation safety management and the application of transportation safety management methods, techniques, processes and practices should be sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples are as follows:

— safety management terminology;

— understanding safe system approach;

— risk assessment and mitigation;

— analysis of human factors related to transportation safety management;

— human behaviour and interaction;

— interaction of humans, machines, processes and the work environment;

— potential hazards and other workplace factors affecting safety;

— methods and practices for incident investigations and monitoring safety performance;

— evaluation of operational incidents and accidents;

— developing proactive and reactive performance measures and metrics.

NOTE For additional information, see the future ISO 39001 developed by ISO/PC 241 on road-traffic safety management systems.

A.3 Illustrative example of discipline-specific knowledge and skills of auditors in environmental management

Knowledge and skills related to the discipline and the application of discipline-specific methods, techniques, processes and practices should be sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples are as follows:

— environmental terminology;

— environmental metrics and statistics;

— measurement science and monitoring techniques;

— interaction of ecosystems and biodiversity;

— environmental media (e.g. air, water, land, fauna, flora);

— techniques for determining risk (e.g. environmental aspects/impacts evaluation, including methods for evaluating significance);

— life cycle assessment;

— environmental performance evaluation;

— pollution prevention and control (e.g. best available techniques for pollution control or energy efficiency);

— source reduction, waste minimization, reuse, recycling and treatment practices and processes;

— use of hazardous substances;

— greenhouse gas emissions accounting and management;

— management of natural resources (e.g. fossil fuels, water, flora and fauna, land);

— environmental design;

— environmental reporting and disclosure;

— product stewardship;

— renewable and low carbon technologies.

NOTE For additional information, see related standards developed by ISO/TC 207 on environmental management.

A.4 Illustrative example of discipline-specific knowledge and skills of auditors in quality management

Knowledge and skills related to the discipline and the application of discipline-specific methods, techniques, processes and practices should be sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples are as follows:

— terminology relating to quality, management, organization, process and product, characteristics, conformity, documentation, audit and measurement processes;

— customer focus, customer-related processes, monitoring and measuring of customer satisfaction, complaints handling, code of conduct, dispute resolution;

— leadership – role of top management, managing for the sustained success of an organization – the quality management approach, realizing financial and economic benefits through management of quality, quality management systems and excellence models;

— involvement of people, human factors, competence, training and awareness;

— process approach, process analysis, capability and control techniques, risk treatment methods;

— system approach to management (rationale of quality management systems, quality management systems and other management system focuses, quality management system documentation), types and value, projects, quality plans, configuration management;

— continual improvement, innovation and learning;

— factual approach to decision making, risk assessment techniques (risk identification, analysis and evaluation), evaluation of quality management (audit, review and self-assessment), measurement and monitoring techniques, requirements for measurement processes and measuring equipment, root cause analysis, statistical techniques;

— characteristics of processes and products, including services;

— mutually beneficial supplier relationships, quality management system requirements and requirements for products, particular requirements for quality management in different sectors.

NOTE For additional information, see related standards developed by ISO/TC 176 on quality management.

A.5 Illustrative example of discipline-specific knowledge and skills of auditors in records management

Knowledge and skills related to the discipline and the application of discipline-specific methods, techniques, processes and practices should be sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples are as follows:

— records, records management processes, and management systems for records terminology;

— developing performance measures and metrics;

— investigation and evaluation of records practices through interviewing, observation and validation;

— sample analysis of records created in business processes. Key characteristics of records, records systems, records processes and controls;

— risk assessment (e.g. assessment of risks through failure to create, maintain and control adequate records of the organization's business processes);

— the performance and adequacy of records processes to create, capture and control records;

— assessment of the adequacy and performance of records systems (including business systems to create and control records), the suitability of technological tools used, and facilities and equipment established;

— evaluation of the different levels of competence in records management required across an organization and the assessment of that competence;

— significance of the content, context, structure, representation and control information (metadata) required to define and manage records and records systems;

— methods for developing records-specific instruments;

— technologies used for creation, capture, conversion and migration, and long-term preservation of electronic/digital records;

— identification and significance of the authorization documentation for records processes.

NOTE For additional information, see related standards developed by ISO/TC 46/SC 11 on records management.

A.6 Illustrative example of discipline-specific knowledge and skills of auditors in resilience, security, preparedness and continuity management

Knowledge and skills related to the discipline and the application of discipline-specific methods, techniques, processes and practices should be sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples are as follows:

— processes, science and technology underlying resilience, security, preparedness, response, continuity and recovery management;

— methods for intelligence gathering and monitoring;

— managing the risks of disruptive events (anticipate, avoid, prevent, protect, mitigate, respond to and recover from a disruptive event);

— risk assessment (asset identification and valuation; and risk identification, analysis, evaluation) and impact analysis (related to human, physical and intangible assets, as well as the environment);

— risk treatment (adaptive, proactive and reactive measures);

— methods and practices for information integrity and sensitivity;

— methods for personnel security and protection of persons;

— methods and practices for asset protection and physical security;

— methods and practices for prevention, deterrence, and security management;

— methods and practices for incident mitigation, response, and crisis management;

— methods and practices for continuity, emergency, and recovery management;

— methods and practices for monitoring, measuring, and reporting of performance (including exercise and testing methodologies).

NOTE For additional information, see related standards developed by ISO/TC 8, ISO/TC 223 and ISO/TC 247 on resilience, security, preparedness and continuity management.

A.7 Illustrative example of discipline-specific knowledge and skills of auditors in information security management

Knowledge and skills related to the discipline and the application of discipline-specific methods, techniques, processes and practices should be sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples are as follows:

— guidelines from standards such as ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005;

— identification and evaluation of customer and interested parties requirements;

— the laws and regulations dealing with information security (e.g. intellectual property; content, protection and retention of organizational records; data protection and privacy; regulation of cryptographic controls; anti-terrorism; electronic commerce; electronic and digital signatures; workplace surveillance; workplace ergonomics; telecommunications interception and monitoring of data (e.g. e-mail), computer abuse, electronic evidence collection, penetration testing, etc.;

— processes, science and technology underlying information security management;

— risk assessment (identification, analysis and evaluation) and trends in technology, threats and vulnerabilities;

— information security risk management;

— methods and practices for information security controls (electronic and physical);

— methods and practices for information integrity and sensitivity;

— methods and practices for measuring and evaluating effectiveness of the information security management system and associated controls;

— methods and practices for measuring, monitoring and recording of performance (including testing, audits and reviews).

NOTE For additional information, see related standards developed by ISO/IEC JTC 1/SC 27 on information security management.

A.8 Illustrative example of discipline-specific knowledge and skills of auditors in occupational health and safety management

A.8.1 General knowledge and skills

Knowledge and skills related to the discipline and the application of discipline-specific methods, techniques, processes and practices should be sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples are as follows:

— hazard identification, including those and other factors affecting human performance in the workplace (such as physical, chemical and biological factors, as well as gender, age, handicap or other physiological, psychological or health factors);

— risk assessment, determining controls, and risk communication [the determining of controls should be based on the “hierarchy of controls” (see OHSAS 18001:2007, 4.3.1)];

— the evaluation of health and human factors (including physiological and psychological factors) and the principles for assessing them;

— method for exposure monitoring and assessment of occupational health and safety risks (including those arising out of the human factors mentioned above or relating to occupational hygiene) and related strategies for eliminating or minimizing such exposures;

— human behaviour, person-to-person interactions and the interaction of humans to machines, processes and the work environment (including workplace, ergonomic and safe design principles, information and communication technologies);

— the evaluation of the different types and levels of occupational health and safety competence required across an organization and the assessment of that competence;

— methods to encourage employee participation and involvement;

— methods to encourage employee wellness or well-being and self-responsibility (in relation to smoking, drugs, alcohol, weight-related issues, exercise, stress, aggressive behaviour, etc.), both during working hours and in their private lives;

— the development, use and evaluation of proactive and reactive performance measures and metrics;

— the principles and practices for identifying potential emergency situations and for emergency planning, prevention, response and recovery;

— methods for incident (including accident and work-related illnesses) investigation and evaluation;

— the determination and use of health-related information (including work-related exposure and illness monitoring data) – but giving special consideration to the confidentiality over particular aspects of such information;

— understanding of medical information (including medical terminology sufficient to understand data related to the prevention of injury and ill-health);

— systems of “occupational exposure limit” values;

— methods for monitoring and reporting on occupational health and safety performance;

— understanding legal and other requirements relevant to occupational health and safety sufficient to enable the auditor to evaluate the occupational health and safety management system.

A.8.2 Knowledge and skills related to the sector being audited

Knowledge and skills related to the sector being audited should be sufficient to enable the auditor to examine the management system within the context of the sector and generate appropriate audit findings and conclusions.

Examples are as follows:

— processes, equipment, raw materials, hazardous substances, process cycles, maintenance, logistics, work flow organization, working practices, shift-scheduling, organizational culture, leadership, behaviour, and other issues specific to the operation or sector;

— typical hazards and risks, including health and human factors, for the sector.

NOTE For additional information see related standards developed by the OHSAS project group on occupational health and safety management.

Annex B
(informative)

Additional guidance for auditors for planning and conducting audits

B.1 Applying audit methods

An audit can be performed using a range of audit methods. An explanation of commonly used audit methods can be found in this annex. The audit methods chosen for an audit depend on the defined audit objectives, scope and criteria, as well as duration and location. Available auditor competence and any uncertainty arising from the application of audit methods should also be considered. Applying a variety and combination of different audit methods can optimize the efficiency and effectiveness of the audit process and its outcome.

Performance of an audit involves an interaction among individuals with the management system being audited and the technology used to conduct the audit. Table B.1 provides examples of audit methods that can be used, singly or in combination, in order to achieve the audit objectives. If an audit involves the use of an audit team with multiple members, both on-site and remote methods may be used simultaneously.

NOTE Additional information about on-site visits is given in Clause B.6.

Table B.1 — Applicable audit methods

Extent of involvement between the auditor and the auditee	Location of the auditor	
	On-site	**Remote**
Human interaction	Conducting interviews. Completing checklists and questionnaires with auditee participation. Conducting document review with auditee participation. Sampling.	Via interactive communication means: — conducting interviews; — completing checklists and questionnaires; — conducting document review with auditee participation.
No human interaction	Conducting document review (e.g. records, data analysis). Observation of work performed. Conducting on-site visit. Completing checklists. Sampling (e.g. products).	Conducting document review (e.g. records, data analysis). Observing work performed via surveillance means, considering social and legal requirements. Analysing data.
On-site audit activities are performed at the location of the auditee. Remote audit activities are performed at any place other than the location of the auditee, regardless of the distance. Interactive audit activities involve interaction between the auditee's personnel and the audit team. Non-interactive audit activities involve no human interaction with persons representing the auditee but do involve interaction with equipment, facilities and documentation.		

The responsibility of the effective application of audit methods for any given audit in the planning stage remains with either the person managing the audit programme or the audit team leader. The audit team leader has this responsibility for conducting the audit activities.

The feasibility of remote audit activities can depend on the level of confidence between auditor and auditee's personnel.

On the level of the audit programme, it should be ensured that the use of remote and on-site application of audit methods is suitable and balanced, in order to ensure satisfactory achievement of audit programme objectives.

B.2 Conducting document review

The auditors should consider if:

— the information in the documents provided is:

  — complete (all expected content is contained in the document);

  — correct (the content conforms to other reliable sources such as standards and regulations);

  — consistent (the document is consistent in itself and with related documents);

  — current (the content is up to date);

— the documents being reviewed cover the audit scope and provide sufficient information to support the audit objectives;

— the use of information and communication technologies, depending on the audit methods, promotes efficient conduct of the audit: specific care is needed for information security due to applicable regulations on protection of data (in particular for information which lies outside the audit scope, but which is also contained in the document).

NOTE Document review can give an indication of the effectiveness of document control within the auditee's management system.

B.3 Sampling

B.3.1 General

Audit sampling takes place when it is not practical or cost effective to examine all available information during an audit, e.g. records are too numerous or too dispersed geographically to justify the examination of every item in the population. Audit sampling of a large population is the process of selecting less than 100 % of the items within the total available data set (population) to obtain and evaluate evidence about some characteristic of that population, in order to form a conclusion concerning the population.

The objective of audit sampling is to provide information for the auditor to have confidence that the audit objectives can or will be achieved.

The risk associated with sampling is that the samples may be not representative of the population from which they are selected, and thus the auditor's conclusion may be biased and be different to that which would be reached if the whole population was examined. There may be other risks depending on the variability within the population to be sampled and the method chosen.

Audit sampling typically involves the following steps:

— establishing the objectives of the sampling plan;

— selecting the extent and composition of the population to be sampled;

— selecting a sampling method;

— determining the sample size to be taken;

— conducting the sampling activity;

— compiling, evaluating, reporting and documenting results.

When sampling, consideration should be given to the quality of the available data, as sampling insufficient and inaccurate data will not provide a useful result. The selection of an appropriate sample should be based on both the sampling method and the type of data required, e.g. to infer a particular behaviour pattern or draw inferences across a population.

Reporting on the sample selected could take into account the sample size, selection method and estimates made based on the sample and the confidence level.

Audits can use either judgement-based sampling (see B.5.2) or statistical sampling (see B.5.3).

B.3.2 Judgement-based sampling

Judgement-based sampling relies on the knowledge, skills and experience of the audit team (see Clause 7).

For judgement-based sampling, the following can be considered:

— previous audit experience within the audit scope;

— complexity of requirements (including legal requirements) to achieve the objectives of the audit;

— complexity and interaction of the organization's processes and management system elements;

— degree of change in technology, human factor or management system;

— previously identified key risk areas and areas of improvement;

— output from monitoring of management systems.

A drawback to judgement-based sampling is that there can be no statistical estimate of the effect of uncertainty in the findings of the audit and the conclusions reached.

B.3.3 Statistical sampling

If the decision is made to use statistical sampling, the sampling plan should be based on the audit objectives and what is known about the characteristics of overall population from which the samples are to be taken.

— Statistical sampling design uses a sample selection process based on probability theory. Attribute-based sampling is used when there are only two possible sample outcomes for each sample (e.g. correct/incorrect or pass/fail). Variable-based sampling is used when the sample outcomes occur in a continuous range.

— The sampling plan should take into account whether the outcomes being examined are likely to be attribute-based or variable-based. For example, when evaluating conformance of completed forms to the requirements set out in a procedure, an attribute-based approach could be used. When examining the occurrence of food safety incidents or the number of security breaches, a variable-based approach would likely be more appropriate.

— The key elements that will affect the audit sampling plan are:

  — the size of the organization;

  — the number of competent auditors;

  — the frequency of audits during the year;

  — the time of individual audit;

  — any externally required confidence level.

— When a statistical sampling plan is developed, the level of sampling risk that the auditor is willing to accept is an important consideration. This is often referred to as the acceptable confidence level. For example, a sampling risk of 5 % corresponds to an acceptable confidence level of 95 %. A sampling risk of 5 % means the auditor is willing to accept the risk that 5 out of 100 (or 1 in 20) of the samples examined will not reflect the actual values that would be seen if the entire population was examined.

— When statistical sampling is used, auditors should appropriately document the work performed. This should include a description of the population that was intended to be sampled, the sampling criteria used for the evaluation (e.g. what is an acceptable sample), the statistical parameters and methods that were utilized, the number of samples evaluated and the results obtained.

B.4 Preparing work documents

When preparing work documents, the audit team should consider the questions below for each document.

a) Which audit record will be created by using this work document?

b) Which audit activity is linked to this particular work document?

c) Who will be the user of this work document?

d) What information is needed to prepare this work document?

For combined audits, work documents should be developed to avoid duplication of audit activities by:

— clustering of similar requirements from different criteria;

— coordinating the content of related checklists and questionnaires.

The work documents should be adequate to address all those elements of the management system within the audit scope and may be provided in any media.

B.5 Selecting sources of information

The sources of information selected may vary according to the scope and complexity of the audit and may include the following:

— interviews with employees and other persons;

— observations of activities and the surrounding work environment and conditions;

— documents, such as policies, objectives, plans, procedures, standards, instructions, licenses and permits, specifications, drawings, contracts and orders;

— records, such as inspection records, minutes of meetings, audit reports, records of monitoring programme and the results of measurements;

— data summaries, analyses and performance indicators;

— information on the auditee's sampling plans and on the procedures for the control of sampling and measurement processes;

— reports from other sources, e.g. customer feedback, external surveys and measurements, other relevant information from external parties and supplier ratings;

— databases and websites;

— simulation and modelling.

B.6 Guidance on visiting the auditee's location

To minimize interference between audit activities and the auditee's work processes and to ensure the health and safety of the audit team during a visit, the following should be considered:

a) planning the visit:

- ensure permission and access to those parts of the auditee's location, to be visited in accordance with the audit scope;
- provide adequate information (e.g. briefing) to auditors on security, health (e.g. quarantine), occupational health and safety matters and cultural norms for the visit including requested and recommended vaccination and clearances, if applicable;
- confirm with the auditee that any required personal protective equipment (PPE) will be available for the audit team, if applicable;
- except for unscheduled ad hoc audits, ensure that personnel being visited will be informed about the audit objectives and scope;

b) on-site activities:

- avoid any unnecessary disturbance of the operational processes;
- ensure that the audit team is using PPE properly;
- ensure emergency procedures are communicated (e.g. emergency exits, assembly points);
- schedule communication to minimize disruption;
- adapt size of the audit team and the number of guides and observers in accordance with the audit scope, in order to avoid interference with the operational processes as far as practicable;
- do not touch or manipulate any equipment, unless explicitly permitted, even when competent or licensed;
- if an incident occurs during the on-site visit, the audit team leader should review the situation with the auditee and, if necessary, with the audit client and reach agreement on whether the audit should be interrupted, rescheduled or continued;
- if taking photographs or video material, ask for authorization from management in advance and consider security and confidentiality matters and avoid taking photographs of individual persons without their permission;
- if taking copies of documents of any kind, ask for permission in advance and consider confidentiality and security matters;
- when taking notes, avoid collecting personal information unless required by the audit objectives or audit criteria.

B.7 Conducting interviews

Interviews are one of the important means of collecting information and should be carried out in a manner adapted to the situation and the person interviewed, either face to face or via other means of communication. However, the auditor should consider the following:

- interviews should be held with persons from appropriate levels and functions performing activities or tasks within the audit scope;
- interviews should normally be conducted during normal working hours and, where practical, at the normal workplace of the person being interviewed;

— attempt to put the person being interviewed at ease prior to and during the interview;

— the reason for the interview and any note taking should be explained;

— interviews may be initiated by asking the persons to describe their work;

— careful selection of the type of question used (e.g. open, closed, leading questions);

— the results from the interview should be summarized and reviewed with the interviewed person;

— the interviewed persons should be thanked for their participation and cooperation.

B.8 Audit findings

B.8.1 Determining audit findings

When determining audit findings, the following should be considered:

— follow-up of previous audit records and conclusions;

— requirements of audit client;

— findings exceeding normal practice, or opportunities for improvement;

— sample size;

— categorization (if any) of the audit findings;

B.8.2 Recording conformities

For records of conformity, the following should be considered:

— identification of the audit criteria against which conformity is shown;

— audit evidence to support conformity;

— declaration of conformity, if applicable.

B.8.3 Recording nonconformities

For records of nonconformity, the following should be considered:

— description of or reference to audit criteria;

— nonconformity declaration;

— audit evidence;

— related audit findings, if applicable.

B.8.4 Dealing with findings related to multiple criteria

During an audit, it is possible to identify findings related to multiple criteria. Where an auditor identifies a finding linked to one criterion on a combined audit, the auditor should consider the possible impact on the corresponding or similar criteria of the other management systems.

Depending on the arrangements with the audit client, the auditor may raise either:

— separate findings for each criterion; or

— a single finding, combining the references to multiple criteria.

Depending on the arrangements with the audit client, the auditor may guide the auditee on how to respond to those findings.

Bibliography

[1] ISO 2859-4, *Sampling procedures for inspection by attributes — Part 4: Procedures for assessment of declared quality levels*

[2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

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

[4] ISO 14001, *Environmental management systems — Requirements with guidance for use*

[5] ISO 14050, *Environmental management — Vocabulary*

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

[7] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[8] ISO 22000, *Food safety management systems — Requirements for any organization in the food chain*

[9] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

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

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

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

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

[15] ISO 28000, *Specification for security management systems for the supply chain*

[16] ISO 30301[1)], *Information and documentation — Management system for records — Requirements*

[17] ISO 31000, *Risk management — Principles and guidelines*

[18] ISO 39001[2)], *Road traffic safety (RTS) management systems — Requirements with guidance for use*

[19] ISO 50001, *Energy management systems — Requirements with guidance for use*

[20] ISO Guide 73:2009, *Risk management — Vocabulary*

[21] OHSAS 18001:2007, *Occupational health and safety management systems — Requirements*

[22] *ISO 9001 Auditing Practices Group* papers available at: www.iso.org/tc176/ISO9001AuditingPracticesGroup

[23] ISO 19011 additional guidelines[2] available at: www.iso.org/19011auditing

1) To be published.

2) Under preparation.

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™