BAHAMAS BUREAU OF STANDARDS AND QUALITY

QUALITY IS OUR STANDARD

FINAL DRAFT BAHAMAS NATIONAL STANDARD

Guidelines for auditing management systems

FDBNS ISO 19011:2018(E)

Bahamas Bureau of Standards & Quality (BBSQ)
Source River Centre, 1000 Bacardi Road
P.O. Box N- 4843, Nassau, New Providence, Bahamas
Tel: (242) 362-1748 thru 55
Fax: (242) 362-9172
Email: standards@bbsq.bs
Website: www.bbsq.bs

NOTICE

Standards are subjected to periodic review.

The next amendment will be sent without charge if you return the self-addressed label. If we do not receive this label we have no record that you wish to be kept up-to-date. Please note amendments are not exclusive of a revision of the document.

Our address:
Bahamas Bureau of Standards & Quality (BBSQ)
Source River Centre
1000 Bacardi Road
P.O. Box N- 4843
Nassau, New Providence
Bahamas

---------- (☐cut along the perforated line☐) ----------

-

BNSXX:20XX

NAME: _____

_____

_____

COMPANY/DESIGNATION:

_____

_____

BBSQ Foreword

"This national standard is identical to the English version of International Standard ISO 90004:2009, ***Quality management — Customer satisfaction — Guidelines for monitoring and measuring***. The national committee responsible for this standard is Technical Committee 9 Management Systems. This standard contains requirements that are relevant for The Bahamas.

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.

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

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

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

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

This document was prepared by Project Committee ISO/PC 302, *Guidelines for auditing management systems.*

This third edition cancels and replaces the second edition (ISO 19011:2011), which has been technically revised.

The main differences compared to the second edition are as follows:

— addition of the risk-based approach to the principles of auditing;

— expansion of the guidance on managing an audit programme, including audit programme risk;

— expansion of the guidance on conducting an audit, particularly the section on audit planning;

— expansion of the generic competence requirements for auditors;

— adjustment of terminology to reflect the process and not the object ("thing");

— removal of the annex containing competence requirements for auditing specific management system disciplines (due to the large number of individual management system standards, it would not be practical to include competence requirements for all disciplines);

— expansion of Annex A to provide guidance on auditing (new) concepts such as organization context, leadership and commitment, virtual audits, compliance and supply chain.

Introduction

Since the second edition of this document was published in 2011, a number of new management system standards have been published, many of which have a common structure, identical core requirements and common terms and core definitions. As a result, there is a need to consider a broader approach to management system auditing, as well as providing guidance that is more generic. Audit results can provide input to the analysis aspect of business planning, and can contribute to the identification of improvement needs and activities.

An audit can be conducted against a range of audit criteria, separately or in combination, including but not limited to:

— requirements defined in one or more management system standards;

— policies and requirements specified by relevant interested parties;

— statutory and regulatory requirements;

— one or more management system processes defined by the organization or other parties;

— management system plan(s) relating to the provision of specific outputs of a management system (e.g. quality plan, project plan).

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

This document concentrates on internal audits (first party) and audits conducted by organizations on their external providers and other external interested parties (second party). This document can also be useful for external audits conducted for purposes other than third party management system certification. ISO/IEC 17021-1 provides requirements for auditing management systems for third party certification; this document can provide useful additional guidance (see Table 1).

Table 1 — Different types of audits

1st party audit	2nd party audit	3rd party audit
Internal audit	External provider audit	Certification and/or accreditation audit
	Other external interested party audit	Statutory, regulatory and similar audit

To simplify the readability of this document, the singular form of "management system" is preferred, but the reader can adapt the implementation of the guidance to their own situation. This also applies to the use of "individual" and "individuals", "auditor" and "auditors".

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

The guidance in this document 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 document 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. The nature and complexity of the organization to be audited, as well as the objectives and scope of the audits to be conducted, should also be considered.

This document adopts the combined audit approach when two or more management systems of different disciplines are audited together. Where these systems are integrated into a single management system, the principles and processes of auditing are the same as for a combined audit (sometimes known as an integrated audit).

This document provides guidance on the management of an audit programme, on the planning and conducting of management system audits, as well as on the competence and evaluation of an auditor and an audit team.

Guidelines for auditing management systems

1 Scope

This document 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. These activities include the individual(s) managing the audit programme, auditors and audit teams.

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

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

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

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

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

3.1
audit
systematic, independent and documented process for obtaining *objective evidence* (3.8) and evaluating it objectively to determine the extent to which the *audit criteria* (3.7) are fulfilled

Note 1 to entry: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself.

Note 2 to entry: External audits include those generally called second and third party audits. Second party audits are conducted by parties having an interest in the organization, such as customers, or by other individuals on their behalf. Third party audits are conducted by independent auditing organizations, such as those providing certification/registration of conformity or governmental agencies.

[SOURCE: ISO 9000:2015, 3.13.1, modified — Notes to entry have been modified]

3.2
combined audit
audit (3.1) carried out together at a single *auditee* (3.13) on two or more *management systems* (3.18)

Note 1 to entry: When two or more discipline-specific management systems are integrated into a single management system this is known as an integrated management system.

[SOURCE: ISO 9000:2015, 3.13.2, modified]

3.3
joint audit
audit (3.1) carried out at a single *auditee* (3.13) by two or more auditing organizations

[SOURCE: ISO 9000:2015, 3.13.3]

3.4
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

[SOURCE: ISO 9000:2015, 3.13.4, modified — wording has been added to the definition]

3.5
audit scope
extent and boundaries of an *audit* (3.1)

Note 1 to entry:The audit scope generally includes a description of the physical and virtual-locations, functions, organizational units, activities and processes, as well as the time period covered.

Note 2 to entry:A virtual location is where an organization performs work or provides a service using an on-line environment allowing individuals irrespective of physical locations to execute processes.

[SOURCE: ISO 9000:2015, 3.13.5, modified — Note 1 to entry has been modified, Note 2 to entry has been added]

3.6
audit plan
description of the activities and arrangements for an *audit* (3.1)

[SOURCE: ISO 9000:2015, 3.13.6]

3.7
audit criteria
set of *requirements* (3.23) used as a reference against which *objective evidence* (3.8) is compared

Note 1 to entry: If the audit criteria are legal (including statutory or regulatory) requirements, the words "compliance" or "non-compliance" are often used in an *audit finding* (3.10).

Note 2 to entry: Requirements may include policies, procedures, work instructions, legal requirements, contractual obligations, etc.

[SOURCE: ISO 9000:2015, 3.13.7, modified — the definition has been changed and Notes to entry 1 and 2 have been added]

3.8
objective evidence
data supporting the existence or verity of something

Note 1 to entry: Objective evidence can be obtained through observation, measurement, test or by other means.

Note 2 to entry: Objective evidence for the purpose of the *audit* (3.1) generally consists of records, statements of fact, or other information which are relevant to the *audit criteria* (3.7) and verifiable.

[SOURCE: ISO 9000:2015, 3.8.3]

3.9
audit evidence
records, statements of fact or other information, which are relevant to the *audit criteria* (3.7) and verifiable

[SOURCE: ISO 9000:2015, 3.13.8]

3.10
audit findings
results of the evaluation of the collected *audit evidence* (3.9) against *audit criteria* (3.7)

Note 1 to entry: Audit findings indicate *conformity* (3.20) or *nonconformity* (3.21).

Note 2 to entry: Audit findings can lead to the identification of risks, opportunities for improvement or recording good practices.

Note 3 to entry: In English if the audit criteria are selected from statutory requirements or regulatory requirements, the audit finding is termed compliance or non-compliance.

[SOURCE: ISO 9000:2015, 3.13.9, modified — Notes to entry 2 and 3 have been modified]

3.11
audit conclusion
outcome of an *audit* (3.1), after consideration of the audit objectives and all *audit findings* (3.10)

[SOURCE: ISO 9000:2015, 3.13.10]

3.12
audit client
organization or person requesting an *audit* (3.1)

Note 1 to entry: In the case of internal audit, the audit client can also be the *auditee* (3.13) or the individual(s) managing the audit programme. Requests for external audit can come from sources such as regulators, contracting parties or potential or existing clients.

[SOURCE: ISO 9000:2015, 3.13.11, modified — Note 1 to entry has been added]

3.13
auditee
organization as a whole or parts thereof being audited

[SOURCE: ISO 9000:2015, 3.13.12, modified]

3.14
audit team
one or more persons conducting an *audit* (3.1), supported if needed by *technical experts* (3.16)

Note 1 to entry: One *auditor* (3.15) of the *audit team* (3.14) is appointed as the audit team leader.

Note 2 to entry: The audit team can include auditors-in-training.

[SOURCE: ISO 9000:2015, 3.13.14]

3.15
auditor
person who conducts an *audit* (3.1)

[SOURCE: ISO 9000:2015, 3.13.15]

3.16
technical expert
<audit> person who provides specific knowledge or expertise to the *audit team* (3.14)

Note 1 to entry: Specific knowledge or expertise relates to the organization, the activity, process, product, service, discipline to be audited, or language or culture.

Note 2 to entry: A technical expert to the *audit team* (3.14) does not act as an *auditor* (3.15).

[SOURCE: ISO 9000:2015, 3.13.16, modified — Notes to entry 1 and 2 have been modified]

3.17
observer
individual who accompanies the *audit team* (3.14) but does not act as an *auditor* (3.15)

[SOURCE: ISO 9000:2015, 3.13.17, modified]

3.18
management system
set of interrelated or interacting elements of an organization to establish policies and objectives, and *processes* (3.24) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines, e.g. quality management, financial management or environmental management.

Note 2 to entry: The management system elements establish the organization's structure, roles and responsibilities, planning, operation, policies, practices, rules, beliefs, objectives and processes to achieve those objectives.

Note 3 to entry: The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

[SOURCE: ISO 9000:2015, 3.5.3, modified — Note 4 to entry has been deleted]

3.19
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected – positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence and likelihood.

Note 3 to entry: Risk is often characterized by reference to potential events (as defined in ISO Guide 73:2009, 3.5.1.3) and consequences (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

[SOURCE: ISO 9000:2015, 3.7.9, modified — Notes to entry 5 and 6 have been deleted]

3.20
conformity
fulfilment of a *requirement* (3.23)

[SOURCE: ISO 9000:2015, 3.6.11, modified — Note 1 to entry has been deleted]

3.21
nonconformity
non-fulfilment of a *requirement* (3.23)

[SOURCE: ISO 9000:2015, 3.6.9, modified — Note 1 to entry has been deleted]

3.22
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO 9000:2015, 3.10.4, modified — Notes to entry have been deleted]

3.23
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in documented information.

[SOURCE: ISO 9000:2015, 3.6.4, modified — Notes to entry 3, 4, 5 and 6 have been deleted]

3.24
process
set of interrelated or interacting activities that use inputs to deliver an intended result

[SOURCE: ISO 9000:2015, 3.4.1, modified — Notes to entry have been deleted]

3.25
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.24), products, services, systems or organizations.

[SOURCE: ISO 9000:2015, 3.7.8, modified — Note 3 to entry has been deleted]

3.26
effectiveness
extent to which planned activities are realized and planned results achieved

[SOURCE: ISO 9000:2015, 3.7.11, modified — Note 1 to entry has been deleted]

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 seven principles outlined below.

a) Integrity: the foundation of professionalism

Auditors and the individual(s) managing an audit programme should:

— perform their work ethically, with honesty and responsibility;

— only undertake audit activities if competent to do so;

— 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 function being audited if practicable. 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 should 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.

g) Risk-based approach: an audit approach that considers risks and opportunities

The risk-based approach should substantively influence the planning, conducting and reporting of audits in order to ensure that audits are focused on matters that are significant for the audit client, and for achieving the audit programme objectives.

5 Managing an audit programme

5.1 General

An audit programme should be established which can include audits addressing one or more management system standards or other requirements, conducted either separately or in combination (combined audit).

The extent of an audit programme should be based on the size and nature of the auditee, as well as on the nature, functionality, complexity, the type of risks and opportunities, and the level of maturity of the management system(s) to be audited.

The functionality of the management system can be even more complex when most of the important functions are outsourced and managed under the leadership of other organizations. Particular attention needs to be paid to where the most important decisions are made and what constitutes the top management of the management system.

In the case of multiple locations/sites (e.g. different countries), or where important functions are outsourced and managed under the leadership of another organization, particular attention should be paid to the design, planning and validation of the audit programme.

In the case of smaller or less complex organizations the audit programme can be scaled appropriately.

In order to understand the context of the auditee, the audit programme should take into account the auditee's:

— organizational objectives;

— relevant external and internal issues;

— the needs and expectations of relevant interested parties;

— information security and confidentiality requirements.

The planning of internal audit programmes and, in some cases programmes for auditing external providers, can be arranged to contribute to other objectives of the organization.

The individual(s) managing the audit programme should ensure the integrity of the audit is maintained and that there is not undue influence exerted over the audit.

Audit priority should be given to allocating resources and methods to matters in a management system with higher inherent risk and lower level of performance.

Competent individuals should be assigned to manage the audit programme.

The audit programme should include information and identify resources to enable the audits to be conducted effectively and efficiently within the specified time frames. The information should include:

a) objectives for the audit programme;

b) risks and opportunities associated with the audit programme (see 5.3) and the actions to address them;

c) scope (extent, boundaries, locations) of each audit within the audit programme;

d) schedule (number/duration/frequency) of the audits;

e) audit types, such as internal or external;

f) audit criteria;

g) audit methods to be employed;

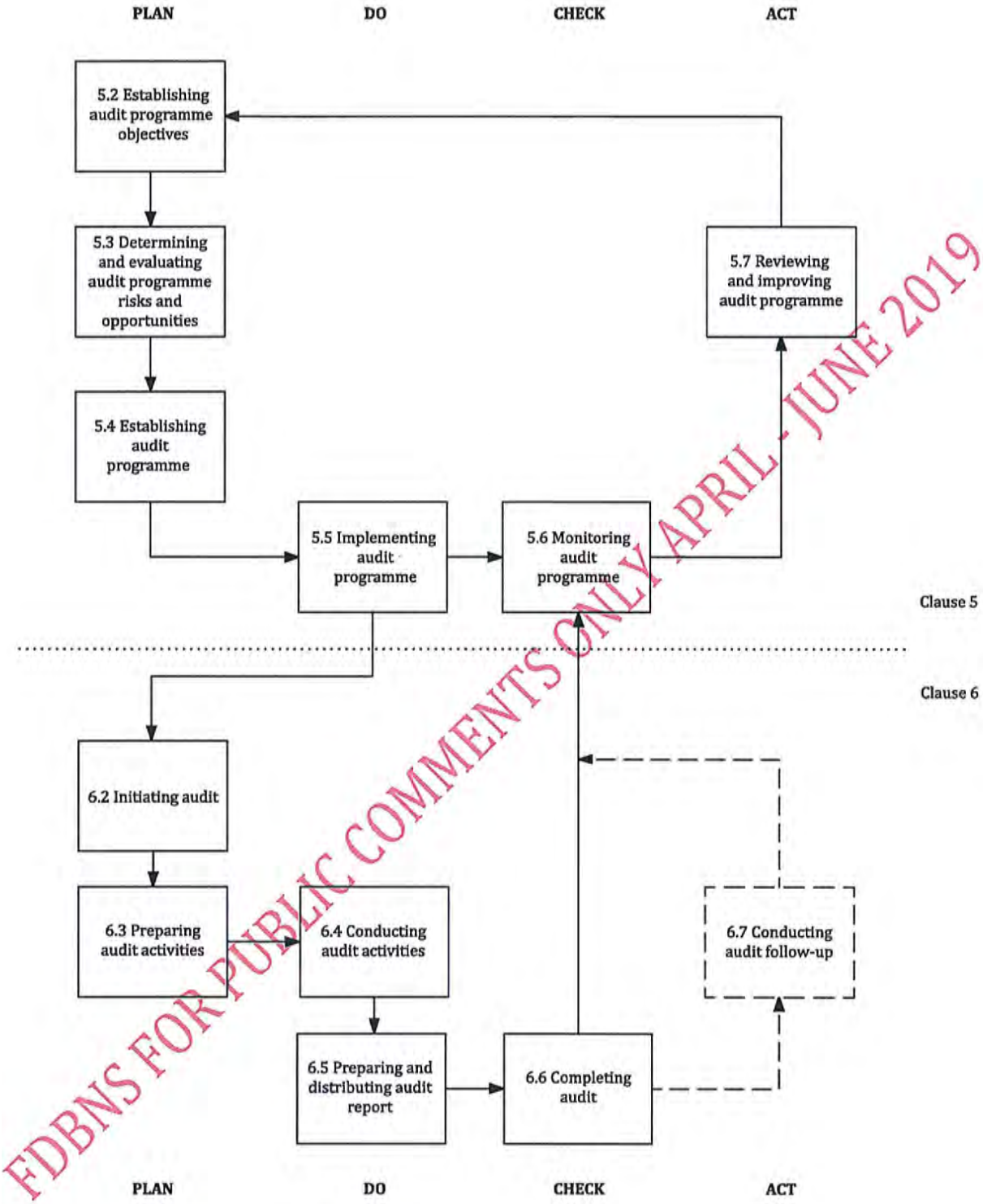
h) criteria for selecting audit team members;

i) relevant documented information.

Some of this information may not be available until more detailed audit planning is complete.

The implementation of the audit programme should be monitored and measured on an ongoing basis (see 5.6) to ensure its objectives have been achieved. The audit programme should be reviewed in order to identify needs for changes and possible opportunities for improvements (see 5.7).

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 document.

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

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

5.2 Establishing audit programme objectives

The audit client should ensure that the audit programme objectives are established to direct the planning and conducting of audits and should ensure the audit programme is implemented effectively. Audit programme objectives should be consistent with the audit client's strategic direction and support management system policy and objectives.

These objectives can be based on consideration of the following:

a) needs and expectations of relevant interested parties, both external and internal;

b) characteristics of and requirements for processes, products, services and projects, and any changes to them;

c) management system requirements;

d) need for evaluation of external providers;

e) auditee's level of performance and level of maturity of the management system(s), as reflected in relevant performance indicators (e.g. KPIs), the occurrence of nonconformities or incidents or complaints from interested parties;

f) identified risks and opportunities to the auditee;

g) results of previous audits.

Examples of audit programme objectives can include the following:

— identify opportunities for the improvement of a management system and its performance;

— evaluate the capability of the auditee to determine its context;

— evaluate the capability of the auditee to determine risks and opportunities and to identify and implement effective actions to address them;

— conform to all relevant requirements, e.g. statutory and regulatory requirements, compliance commitments, requirements for certification to a management system standard;

— obtain and maintain confidence in the capability of an external provider;

— determine the continuing suitability, adequacy and effectiveness of the auditee's management system;

— evaluate the compatibility and alignment of the management system objectives with the strategic direction of the organization.

5.3 Determining and evaluating audit programme risks and opportunities

There are risks and opportunities related to the context of the auditee that can be associated with an audit programme and can affect the achievement of its objectives. The individual(s) managing the audit programme should identify and present to the audit client the risks and opportunities considered when developing the audit programme and resource requirements, so that they can be addressed appropriately.

There can be risks associated with the following:

a) planning, e.g. failure to set relevant audit objectives and determine the extent, number, duration, locations and schedule of the audits;

b) resources, e.g. allowing insufficient time, equipment and/or training for developing the audit programme or conducting an audit;

c) selection of the audit team, e.g. insufficient overall competence to conduct audits effectively;

d) communication, e.g. ineffective external/internal communication processes/channels;

e) implementation, e.g. ineffective coordination of the audits within the audit programme, or not considering information security and confidentiality;

f) control of documented information, e.g. ineffective determination of the necessary documented information required by auditors and relevant interested parties, failure to adequately protect audit records to demonstrate audit programme effectiveness;

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

h) availability and cooperation of auditee and availability of evidence to be sampled.

Opportunities for improving the audit programme can include:

— allowing multiple audits to be conducted in a single visit;

— minimizing time and distances travelling to site;

— matching the level of competence of the audit team to the level of competence needed to achieve the audit objectives;

— aligning audit dates with the availability of auditee's key staff.

5.4 Establishing the audit programme

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

The individual(s) managing the audit programme should:

a) establish the extent of the audit programme according to the relevant objectives (see 5.2) and any known constraints;

b) determine the external and internal issues, and risks and opportunities that can affect the audit programme, and implement actions to address them, integrating these actions in all relevant auditing activities, as appropriate;

c) ensuring the selection of audit teams and the overall competence for the auditing activities by assigning roles, responsibilities and authorities, and supporting leadership, as appropriate;

d) establish all relevant processes including processes for:

— the coordination and scheduling of all audits within the audit programme;

— the establishment of audit objectives, scope(s) and criteria of the audits, determining audit methods and selecting the audit team;

— evaluating auditors;

— the establishment of external and internal communication processes, as appropriate;

— the resolutions of disputes and handling of complaints;

— audit follow-up if applicable;

— reporting to the audit client and relevant interested parties, as appropriate.

e) determine and ensure provision of all necessary resources;

f) ensure that appropriate documented information is prepared and maintained, including audit programme records;

g) monitor, review and improve the audit programme;

h) communicate the audit programme to the audit client and, as appropriate, relevant interested parties.

The individual(s) managing the audit programme should request its approval by the audit client.

5.4.2 Competence of individual(s) managing audit programme

The individual(s) managing the audit programme should have the necessary competence to manage the programme and its associated risks and opportunities and external and internal issues effectively and efficiently, including knowledge of:

a) audit principles (see Clause 4), methods and processes (see A.1 and A.2);

b) management system standards, other relevant standards and reference/guidance documents;

c) information regarding the auditee and its context (e.g. external/internal issues, relevant interested parties and their needs and expectations, business activities, products, services and processes of the auditee);

d) applicable statutory and regulatory requirements and other requirements relevant to the business activities of the auditee.

As appropriate, knowledge of risk management, project and process management, and information and communications technology (ICT) may be considered.

The individual(s) managing the audit programme should engage in appropriate continual development activities to maintain the necessary competence to manage the audit programme.

5.4.3 Establishing extent of audit programme

The individual(s) managing the audit programme should determine the extent of the audit programme. This can vary depending on the information provided by the auditee regarding its context (see 5.3).

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 or organization).

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

a) the objective, scope and duration of each audit and the number of audits to be conducted, reporting method and, if applicable, audit follow up;

b) the management system standards or other applicable criteria;

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

d) those factors influencing the effectiveness of the management system;

e) applicable audit criteria, such as planned arrangements for the relevant management system standards, statutory and regulatory requirements and other requirements to which the organization is committed;

f) results of previous internal or external audits and management reviews, if appropriate;

g) results of a previous audit programme review;

h) language, cultural and social issues;

i) the concerns of interested parties, such as customer complaints, non-compliance with statutory and regulatory requirements and other requirements to which the organization is committed, or supply chain issues;

j) significant changes to the auditee's context or its operations and related risks and opportunities;

k) availability of information and communication technologies to support audit activities, in particular the use of remote audit methods (see A.16);

l) the occurrence of internal and external events, such as nonconformities of products or service, information security leaks, health and safety incidents, criminal acts or environmental incidents;

m) business risks and opportunities, including actions to address them.

5.4.4 Determining audit programme resources

When determining resources for the audit programme, the individual(s) managing the audit programme should consider:

a) the financial and time resources necessary to develop, implement, manage and improve audit activities;

b) audit methods (see A.1);

c) the individual and overall availability of auditors and technical experts having competence appropriate to the particular audit programme objectives;

d) the extent of the audit programme (see 5.4.3) and audit programme risks and opportunities (see 5.3);

e) travel time and cost, accommodation and other auditing needs;

f) the impact of different time zones;

g) the availability of information and communication technologies (e.g. technical resources required to set up a remote audit using technologies that support remote collaboration);

h) the availability of any tools, technology and equipment required;

i) the availability of necessary documented information, as determined during the establishment of the audit programme (see A.5);

j) requirements related to the facility, including any security clearances and equipment (e.g. background checks, personal protective equipment, ability to wear clean room attire).

5.5 Implementing audit programme

5.5.1 General

Once the audit programme has been established (see 5.4.3) and related resources have been determined (see 5.4.4) it is necessary to implement the operational planning and the coordination of all the activities within the programme.

The individual(s) managing the audit programme should:

a) communicate the relevant parts of the audit programme, including the risks and opportunities involved, to relevant interested parties and inform them periodically of its progress, using established external and internal communication channels;

b) define objectives, scope and criteria for each individual audit;

c) select audit methods (see A.1);

d) coordinate and schedule audits and other activities relevant to the audit programme;

e) ensure the audit teams have the necessary competence (see 5.5.4);

f) provide necessary individual and overall resources to the audit teams (see 5.4.4);

g) ensure the conduct of audits in accordance with the audit programme, managing all operational risks, opportunities and issues (i.e. unexpected events), as they arise during the deployment of the programme;

h) ensure relevant documented information regarding the auditing activities is properly managed and maintained (see 5.5.7);

i) define and implement the operational controls (see 5.6) necessary for audit programme monitoring;

j) review the audit programme in order to identify opportunities for its improvement (see 5.7).

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

Each individual audit should be based on defined audit objectives, scope and criteria. These should 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:

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

b) evaluation of the capability of the management system to assist the organization in meeting relevant statutory and regulatory requirements and other requirements to which the organization is committed;

c) evaluation of the effectiveness of the management system in meeting its intended results;

d) identification of opportunities for potential improvement of the management system;

e) evaluation of the suitability and adequacy of the management system with respect to the context and strategic direction of the auditee;

f) evaluation of the capability of the management system to establish and achieve objectives and effectively address risks and opportunities, in a changing context, including the implementation of the related actions.

The audit scope should be consistent with the audit programme and audit objectives. It includes such factors as locations, functions, 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. These may include one or more of the following: applicable policies, processes, procedures, performance criteria including objectives, statutory and regulatory requirements, management system requirements, information regarding the context and the risks and opportunities as determined by the auditee (including relevant external/internal interested parties 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 and communicated to interested parties, for approval if appropriate.

When more than one discipline is being audited at the same time it is important that the audit objectives, scope and criteria are consistent with the relevant audit programmes for each discipline. Some disciplines can have a scope that reflects the whole organization and others can have a scope that reflects a subset of the whole organization.

5.5.3 Selecting and determining audit methods

The individual(s) managing the audit programme should select and determine the methods for effectively and efficiently conducting an audit, depending on the defined audit objectives, scope and criteria.

Audits can be performed on-site, remotely or as a combination. The use of these methods should be suitably balanced, based on, among others, consideration of associated risks and opportunities.

Where two or more auditing organizations conduct a joint audit of the same auditee, the individuals managing the different audit programmes should agree on the audit methods 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.

5.5.4 Selecting audit team members

The individual(s) 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.

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

— identification of the competence needed to achieve the objectives of the audit;

— selection of the audit team members so that the necessary competence is present in the audit team.

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;

c) whether the audit is a combined or joint audit;

d) the selected audit methods;

e) ensuring objectivity and impartiality to avoid any conflict of interest of the audit process;

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

g) the relevant external/internal issues, such as 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, also considering the need for interpreters;

h) type and complexity of the processes to be audited.

Where appropriate, the individual(s) managing the audit programme should consult the team leader on the composition of the audit team.

If the necessary competence is not covered by the auditors in the audit team, technical experts with additional competence should be made available to support the team.

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

Changes to the composition of the audit team may be necessary during the audit, e.g. if a conflict of interest or competence issue arises. If such a situation arises, it should be resolved with the appropriate parties (e.g. audit team leader, the individual(s) managing the audit programme, audit client or auditee) before any changes are made.

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

The individual(s) 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 relevant documented information;

c) audit scope, including identification of the organization and its functions and processes to be audited;

d) audit processes and associated methods;

e) composition of the audit team;

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

g) resources necessary to conduct the audit;

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

i) information which supports the audit team leader(s) in their interactions with the auditee for the effectiveness of the audit programme.

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 reporting output as required and to whom it is to be distributed;

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

— any health, safety and environmental arrangements for the auditors;

— requirements for travel or access to remote sites;

— any security and authorization requirements;

— any actions to be reviewed, e.g. follow-up actions from a previous audit;

— coordination with other audit activities, e.g. when different teams are auditing similar or related processes at different locations or 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.

5.5.6 Managing audit programme results

The individual(s) managing the audit programme should ensure that the following activities are performed:

a) evaluation of the achievement of the objectives for each audit within the audit programme;

b) review and approval of audit reports regarding the fulfilment of the audit scope and objectives;

c) review of the effectiveness of actions taken to address audit findings;

d) distribution of audit reports to relevant interested parties;

e) determination of the necessity for any follow-up audit.

The individual managing the audit programme should consider, where appropriate:

— communicating audit results and best practices to other areas of the organization, and

— the implications for other processes.

5.5.7 Managing and maintaining audit programme records

The individual(s) managing the audit programme should ensure that audit records are generated, managed and maintained to demonstrate the implementation of the audit programme. Processes should be established to ensure that any information security and confidentiality needs associated with the audit records are addressed.

Records can include the following:

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

- schedule of audits;
- audit programme objectives and extent;
- those addressing audit programme risks and opportunities, and relevant external and internal issues;
- reviews of the audit programme effectiveness.

b) Records related to each audit, such as:

- audit plans and audit reports;
- objective audit evidence and findings;
- nonconformity reports;
- corrections and corrective action reports;
- audit follow-up reports.

c) Records related to the audit team covering topics such as:

- competence and performance evaluation of the audit team members;
- criteria for the selection of audit teams and team members and formation of audit teams;
- 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.

5.6 Monitoring audit programme

The individual(s) managing the audit programme should ensure the evaluation of:

a) whether schedules are being met and audit programme objectives are being achieved;

b) the performance of the audit team members including the audit team leader and the technical experts;

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

d) feedback from audit clients, auditees, auditors, technical experts and other relevant parties;

e) sufficiency and adequacy of documented information in the whole audit process.

Some factors can indicate the need to modify the audit programme. These can include changes to:

— audit findings;

— demonstrated level of auditee's management system effectiveness and maturity;

— effectiveness of the audit programme;

— audit scope or audit programme scope;

— the auditee's management system;

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

— external providers;

— identified conflicts of interest;

— the audit client's requirements.

5.7 Reviewing and improving audit programme

The individual(s) managing the audit programme and the audit client 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 improvement of the programme.

The individual(s) managing the audit programme should ensure the following:

— review of the overall implementation of the audit programme;

— identification of areas and opportunities for improvement;

— application of changes to the audit programme if necessary;

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

— reporting of the results of the audit programme and review with the audit client and relevant interested parties, as appropriate.

The audit programme review should consider the following:

a) results and trends from audit programme monitoring;

b) conformity with audit programme processes and relevant documented information;

c) evolving needs and expectations of relevant interested parties;

d) audit programme records;

e) alternative or new auditing methods;

f) alternative or new methods to evaluate auditors;

g) effectiveness of the actions to address the risks and opportunities, and internal and external issues associated with the audit programme;

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

6 Conducting an audit

6.1 General

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

6.2 Initiating audit

6.2.1 General

The responsibility for conducting the audit should remain with the assigned audit team leader (see 5.5.5) until the audit is completed (see 6.6).

To initiate an audit, the steps in Figure 1 should be considered; however, the sequence can differ depending on the auditee, processes and specific circumstances of the audit.

6.2.2 Establishing contact with auditee

The audit team leader should ensure that contact is made with the auditee to:

a) confirm communication channels with the auditee's representatives;

b) confirm the authority to conduct the audit;

c) provide relevant information on the audit objectives, scope, criteria, methods and audit team composition, including any technical experts;

d) request access to relevant information for planning purposes including information on the risks and opportunities the organization has identified and how they are addressed;

e) determine applicable statutory and regulatory requirements and other requirements relevant to the activities, processes, products and services of the auditee;

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

g) make arrangements for the audit including the schedule;

h) determine any location-specific arrangements for access, health and safety, security, confidentiality or other;

i) agree on the attendance of observers and the need for guides or interpreters for the audit team;

j) determine any areas of interest, concern or risks to the auditee in relation to the specific audit;

k) resolve issues regarding composition of the audit team with the auditee or audit client.

6.2.3 Determining feasibility of 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 factors such as the availability of the following:

a) sufficient and appropriate information for planning and conducting the audit;

b) adequate cooperation from the auditee;

c) adequate time and resources for conducting the audit.

NOTE Resources include access to adequate and appropriate information and communication technology.

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 review of documented information

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

— gather information to understand the auditee's operations and to prepare audit activities and applicable audit work documents (see 6.3.4), e.g. on processes, functions;

— establish an overview of the extent of the documented information to determine possible conformity to the audit criteria and detect possible areas of concern, such as deficiencies, omissions or conflicts.

The documented information should include, but not be limited to: management system documents and records, as well as previous audit reports. The review should take into account the context of the auditee's organization, including its size, nature and complexity, and its related risks and opportunities. It should also take into account the audit scope, criteria and objectives.

NOTE Guidance on how to verify information is provided in A.5.

6.3.2 Audit planning

6.3.2.1 Risk-based approach to planning

The audit team leader should adopt a risk-based approach to planning the audit based on the information in the audit programme and the documented information provided by the auditee.

Audit planning should consider the risks 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. Planning 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 risk of not achieving the audit objectives. In planning the audit, the audit team leader should consider the following:

a) the composition of the audit team and its overall competence;

b) the appropriate sampling techniques (see A.6);

c) opportunities to improve the effectiveness and efficiency of the audit activities;

d) the risks to achieving the audit objectives created by ineffective audit planning;

e) the risks to the auditee created by performing the audit.

Risks to the auditee can result from the presence of the audit team members adversely influencing the auditee's arrangements for health and safety, environment and quality, and its 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 any competing objectives and priorities of the different management systems.

6.3.2.2 Audit planning details

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

Audit planning should address or reference the following:

a) the audit objectives;

b) the audit scope, including identification of the organization and its functions, as well as processes to be audited;

c) the audit criteria and any reference documented information;

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

e) the need for the audit team to familiarize themselves with auditee's facilities and processes (e.g. by conducting a tour of physical location(s), or reviewing information and communication technology);

f) the audit methods to be used, including the extent to which audit sampling is needed to obtain sufficient audit evidence;

g) the roles and responsibilities of the audit team members, as well as guides and observers or interpreters;

h) the allocation of appropriate resources based upon consideration of the risks and opportunities related to the activities that are to be audited.

Audit planning should take into account, as appropriate:

— identification of the auditee's representative(s) 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 actions to be taken to address risks to achieving the audit objectives and opportunities arising;

— matters related to confidentiality and information security;

— any follow-up actions from a previous audit or other source(s) e.g. lessons learned, project reviews;

— any follow-up activities to the planned audit;

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

Audit plans should be presented to the auditee. Any issues with the audit plans should be resolved between the audit team leader, the auditee and, if necessary, the individual(s) managing the audit programme.

6.3.3 Assigning work to 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 and, as appropriate, authority for decision-making. Such assignments should take into account the impartiality and objectivity 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 meetings 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 documented information for audit

The audit team members should collect and review the information relevant to their audit assignments and prepare documented information for the audit, using any appropriate media. The documented information for the audit can include but is not limited to:

a) physical or digital checklists;

b) audit sampling details;

c) audio visual information.

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

NOTE Guidance on preparing audit work documents is given in A.13.

Documented information prepared for, and resulting from, the audit should be retained at least until audit completion, or as specified in the audit programme. Retention of documented information after audit completion is described in 6.6. Documented information created during the audit process involving confidential or proprietary information should be suitably safeguarded at all times by the audit team members.

6.4 Conducting audit activities

6.4.1 General

Audit activities are normally conducted in a defined sequence as indicated in Figure 1. This sequence may be varied to suit the circumstances of specific audits.

6.4.2 Assigning roles and responsibilities of guides and observers

Guides and observers may accompany the audit team with approvals from the audit team leader, audit client and/or auditee, if required. 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 being present during certain audit activities.

For observers, any arrangements for access, health and safety, environmental, 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 or the auditor to which they have been assigned. Their responsibilities should include the following:

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

b) arranging access to specific locations of the auditee;

c) ensuring that rules concerning location-specific arrangements for access, health and safety, environmental, security, confidentiality and other issues are known and respected by the audit team members and observers and any risks are addressed;

d) witnessing the audit on behalf of the auditee, when appropriate;

e) providing clarification or assisting in collecting information, when needed.

6.4.3 Conducting opening meeting

The purpose of the opening meeting is to:

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

b) introduce the audit team and their roles;

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 retained. The meeting should be chaired by the audit team leader.

Introduction of the following should be considered, as appropriate:

— other participants, including observers and guides, interpreters and an outline of their roles;

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

Confirmation of the following items should be considered, as appropriate:

— the audit objectives, scope and criteria;

— 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 change(s) needed;

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

— the language to be used during the audit;

— the auditee being kept informed of audit progress during the audit;

— the availability of the resources and facilities needed by the audit team;

— matters relating to confidentiality and information security;

— relevant access, health and safety, security, emergency and other arrangements for the audit team;

— activities on site that can impact the conduct of the audit.

The presentation of information on the following items should be considered, as appropriate:

— the method of reporting audit findings including criteria for grading, if any;

— conditions under which the audit may be terminated;

— how to deal with possible findings during the audit;

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

6.4.4 Communicating during 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 interested parties (e.g. regulators), especially where statutory and regulatory requirements require mandatory reporting of nonconformities.

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, any significant findings and any concerns to the auditee and audit client, as appropriate. Evidence collected during the audit that suggests an immediate and significant risk 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 changes to audit planning, 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 accepted, as appropriate, by both the individual(s) managing the audit programme and the audit client, and presented to the auditee.

6.4.5 Audit information availability and access

The audit methods chosen for an audit depend on the defined audit objectives, scope and criteria, as well as duration and location. The location is where the information needed for the specific audit activity is available to the audit team. This may include physical and virtual locations.

Where, when and how to access audit information is crucial to the audit. This is independent of where the information is created, used and/or stored. Based on these issues, the audit methods need to be

determined (see Table A.1). The audit can use a mixture of methods. Also, audit circumstances may mean that the methods need to change during the audit.

6.4.6 Reviewing documented information while conducting audit

The auditee's relevant documented information 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 verify information is provided in A.5.

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 documented information cannot be provided within the time frame given in the audit plan, the audit team leader should inform both the individual(s) 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 documented information concerns are resolved.

6.4.7 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, as far as practicable.

NOTE 1 For verifying information see A.5.

NOTE 2 Guidance on sampling is given in A.6.

Only information that can be subject to some degree of verification should be accepted as audit evidence. Where the degree of verification is low the auditor should use their professional judgement to determine the degree of reliance that can be placed on it as evidence. Audit evidence leading to audit findings should be recorded. If, during the collection of objective evidence, the audit team becomes aware of any new or changed circumstances, or risks or opportunities, these should be addressed by the team accordingly.

Figure 2 provides an overview of a typical process, from collecting information to reaching audit conclusions.

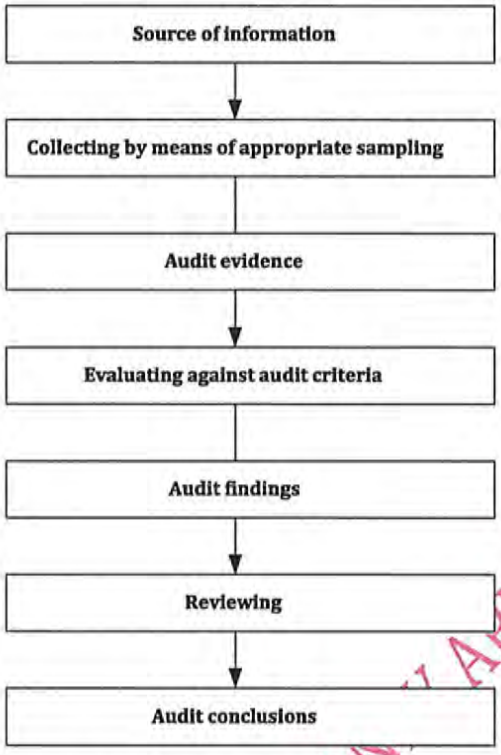


Figure 2 — Overview of a typical process of collecting and verifying information

Methods of collecting information include, but are not limited to the following:

— interviews;

— observations;

— review of documented information.

NOTE 3 Guidance on selecting sources of information and observation is given in A.14.

NOTE 4 Guidance on visiting the auditee's location is given in A.15.

NOTE 5 Guidance on conducting interviews is given in A.17.

6.4.8 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 can be graded depending on the context of the organization and its risks. This grading can be quantitative (e.g. 1 to 5) and qualitative (e.g. minor, major). 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. Unresolved issues should be recorded in the audit report.

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

NOTE 1 Additional guidance on the identification and evaluation of audit findings is given in A.18.

NOTE 2 Conformity or nonconformity with audit criteria related to statutory or regulatory requirements or other requirements, is sometimes referred to as compliance or non-compliance.

6.4.9 Determining audit conclusions

6.4.9.1 Preparation for closing meeting

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.

6.4.9.2 Content of audit conclusions

Audit conclusions should address issues such as the following:

a) the extent of conformity with the audit criteria and robustness of the management system, including the effectiveness of the management system in meeting the intended outcomes, the identification of risks and effectiveness of actions taken by the auditee to address risks;

b) the effective implementation, maintenance and improvement of the management system;

c) achievement of audit objectives, coverage of audit scope and fulfilment of audit criteria;

d) similar findings made in different areas that were audited or from a joint or previous audit for the purpose of identifying trends.

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

6.4.10 Conducting closing meeting

A closing meeting should be held to present the audit findings and conclusions.

The closing meeting should be chaired by the audit team leader and attended by the management of the auditee and include, as applicable:

— those responsible for the functions or processes which have been audited;

— the audit client;

— other members of the audit team;

— other relevant interested parties as determined by the audit client and/or auditee.

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 take into account the effectiveness of the management system in achieving the auditee's objectives, including consideration of its context and risks and opportunities.

The familiarity of the auditee with the audit process should also be taken into consideration during the closing meeting, to ensure the correct level of detail is provided to participants.

For some audit situations, the meeting can be formal and minutes, including records of attendance, should be kept. In other instances, e.g. internal audits, the closing meeting can be less formal and consist solely of communicating the audit findings and audit conclusions.

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

a) advising that the audit evidence collected was based on a sample of the information available and is not necessarily fully representative of the overall effectiveness of the auditee's processes;

b) the method of reporting;

c) how the audit finding should be addressed based on the agreed process;

d) possible consequences of not adequately addressing the audit findings;

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

f) any related post-audit activities (e.g. implementation and review of corrective actions, addressing audit complaints, 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, opportunities for improvement recommendations may be presented. It should be emphasized that recommendations are not binding.

6.5 Preparing and distributing audit report

6.5.1 Preparing audit report

The audit team leader should report the audit conclusions in accordance with the audit programme. The audit report should provide a complete, accurate, concise and clear record of the audit, and should include or refer to the following:

a) audit objectives;

b) audit scope, particularly identification of the organization (the auditee) and the functions or processes audited;

c) identification of the audit client;

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

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

f) audit criteria;

g) audit findings and related evidence;

h) audit conclusions;

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

j) any unresolved diverging opinions between the audit team and the auditee;

k) audits by nature are a sampling exercise; as such there is a risk that the audit evidence examined is not representative.

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 including any issues of availability of evidence, resources or confidentiality, with related justifications;

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

— good practices identified;

— agreed action plan follow-up, if any;

— a statement of the confidential nature of the contents;

— any implications for the audit programme or subsequent audits.

6.5.2 Distributing 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 individual(s) managing the audit programme.

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

The audit report should then be distributed to the relevant interested parties defined in the audit programme or audit plan.

When distributing the audit report, appropriate measures to ensure confidentiality should be considered.

6.6 Completing 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 audit plan).

Documented information pertaining to the audit should be retained or disposed of by agreement between the participating parties and in accordance with audit programme and applicable requirements.

Unless required by law, the audit team and the individual(s) managing the audit programme should not disclose any 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 can identify risks and opportunities for the audit programme and the auditee.

6.7 Conducting audit follow-up

The outcome of the audit can, depending on the audit objectives, indicate the need for corrections, or for corrective actions, or opportunities for improvement. Such actions are usually decided and undertaken by the auditee within an agreed timeframe. As appropriate, the auditee should keep the individual(s) managing the audit programme and/or 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. Outcomes should be reported to the individual managing the audit programme and reported to the audit client for management review.

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 performing audits, including auditors and audit team leaders. Competence should be evaluated regularly 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 to provide an outcome that is objective, consistent, fair and reliable. The evaluation process should include four main steps, as follows:

a) determine the required competence 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 5.5.4);

— 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 7.3, 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 as well as the criteria established in 7.1.

The competence required of the individual(s) managing the audit programme is described in 5.4.2.

7.2 Determining auditor competence

7.2.1 General

In deciding the necessary competence for an audit, an auditor's knowledge and skills related to the following should be considered:

a) the size, nature, complexity, products, services and processes of auditees;

b) the methods for auditing;

c) the management system disciplines to be audited;

d) the complexity and processes of the management system to be audited;

e) the types and levels of risks and opportunities addressed by the management system;

f) the objectives and extent of the audit programme;

g) the uncertainty in achieving audit objectives;

h) other requirements, such as those imposed by the audit client or other relevant interested parties, where appropriate.

This information should be matched against that listed in 7.2.3.

7.2.2 Personal behaviour

Auditors should possess the necessary attributes 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. Desired professional behaviours include being:

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

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

c) diplomatic, i.e. tactful in dealing with individuals;

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

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

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

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

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

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

j) able to act 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;

k) open to improvement, i.e. willing to learn from situations;

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

m) 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:

a) the knowledge and skills necessary to achieve the intended results of the audits they are expected to perform;

b) generic competence and a level of 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, processes and methods: knowledge and skills in this area enable the auditor to ensure audits are performed in a consistent and systematic manner.

   An auditor should be able to:

   — understand the types of risks and opportunities associated with auditing and the principles of the risk-based approach to auditing;

   — plan and organize the work effectively;

   — perform the audit within the agreed time schedule;

   — prioritize and focus on matters of significance;

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

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

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

   — understand and consider technical experts' opinions;

   — audit a process from start to finish, including the interrelations with other processes and different functions, where appropriate;

   — 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;

— document audit activities and audit findings, and prepare reports;

— maintain the confidentiality and security of information.

b) Management system standards and other references: knowledge and skills in this area enable the auditor to understand the audit scope and apply audit criteria, and should cover the following:

— management system standards or other normative or guidance/supporting documents used to establish audit criteria or methods;

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

— relationships and interactions between the management system(s) processes;

— understanding the importance and priority of multiple standards or references;

— application of standards or references to different audit situations.

c) The organization and its context: knowledge and skills in this area enable the auditor to understand the auditee's structure, purpose and management practices and should cover the following:

— needs and expectations of relevant interested parties that impact the management system;

— type of organization, governance, size, structure, functions and relationships;

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

— cultural and social aspects of the auditee.

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

— statutory and regulatory requirements and their governing agencies;

— basic legal terminology;

— contracting and liability.

NOTE Awareness of statutory and regulatory requirements does not imply legal expertise and a management system audit should not be treated as a legal compliance audit.

7.2.3.3 Discipline and sector-specific competence of auditors

Audit teams should have the collective discipline and sector-specific competence appropriate for auditing the particular types of management systems and sectors.

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

a) management system requirements and principles, and their application;

b) fundamentals of the discipline(s) and sector(s) related to the management systems standards as applied by the auditee;

c) application of discipline and sector-specific methods, techniques, processes and practices to enable the audit team to assess conformity within the defined audit scope and generate appropriate audit findings and conclusions;

d) principles, methods and techniques relevant to the discipline and sector, such that the auditor can determine and evaluate the risks and opportunities associated with the audit objectives.

7.2.3.4 Generic competence of audit team leader

In order to facilitate the efficient and effective conduct of the audit an audit team leader should have the competence to:

a) plan the audit and assign audit tasks according to the specific competence of individual audit team members;

b) discuss strategic issues with top management of the auditee to determine whether they have considered these issues when evaluating their risks and opportunities;

c) develop and maintain a collaborative working relationship among the audit team members;

d) manage the audit process, including:

- 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 and safety, and security arrangements;
- directing the audit team members;
- providing direction and guidance to auditors-in-training;
- preventing and resolving conflicts and problems that can occur during the audit, including those within the audit team, as necessary.

e) represent the audit team in communications with the individual(s) managing the audit programme, the audit client and the auditee;

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

g) prepare and complete the audit report.

7.2.3.5 Knowledge and skills for auditing multiple disciplines

When auditing multiple discipline management systems, the audit team member should have an understanding of the interactions and synergy between the different management systems.

Audit team leaders should understand the requirements of each of the management system standards being audited and recognize the limits of their competence in each of the disciplines.

NOTE Audits of multiple disciplines done simultaneously can be done as a combined audit or as an audit of an integrated management system that covers multiple disciplines.

7.2.4 Achieving auditor competence

Auditor competence can be acquired using a combination of the following:

a) successfully completing training programmes that cover generic auditor knowledge and skills;

b) 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 relevant interested parties;

c) education/training and experience in a specific management system discipline and sector that contribute to the development of overall competence;

d) audit experience acquired under the supervision of an auditor competent in the same discipline.

NOTE Successful completion of a training course will depend on the type of course. For courses with an examination component it can mean successfully passing the examination. For other courses, it can mean participating in and completing the course.

7.2.5 Achieving audit team leader competence

An audit team leader should have acquired additional audit experience to develop the competence described in 7.2.3.4. This additional experience should have been gained by working under the direction and guidance of a different audit team leader.

7.3 Establishing auditor evaluation criteria

The criteria should be qualitative (such as having demonstrated desired 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 appropriate auditor evaluation method

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

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

b) the various methods outlined may differ in their reliability;

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

Table 2 — Auditor 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 auditing experience
Feedback	To provide information about how the performance of the auditor is perceived	Surveys, questionnaires, personal references, testimonials, complaints, performance evaluation, peer review

Evaluation method	Objectives	Examples
Interview	To evaluate desired professional behaviour and communication skills, to verify information and test knowledge and to acquire additional information	Personal interviews
Observation	To evaluate desired professional behaviour and the ability to apply knowledge and skills	Role playing, witnessed audits, on-the-job performance
Testing	To evaluate desired 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 opportunities for improvement	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 auditor under evaluation should be compared against the criteria set in 7.2.3. When an auditor under evaluation who is 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. 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 individual(s) 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:

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

b) developments in the practice of auditing including the use of technology;

c) relevant standards including guidance/supporting documents and other requirements;

d) changes in sector or disciplines.

Annex A
(informative)

Additional guidance for auditors planning and conducting audits

A.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 within the management system being audited and the technology used to conduct the audit. Table A.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 on visiting physical locations is given in A.15.

Table A.1 — 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; — observing work performed with remote guide; — completing checklists and questionnaires; — conducting document review with auditee participation.
No human interaction	Conducting document review (e.g. records, data analysis) Observing 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 statutory and regulatory 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 individuals 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 individual(s) 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 several factors (e.g. the level of risk to achieving the audit objectives, the level of confidence between auditor and auditee's personnel and regulatory requirements).

At 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.

A.2 Process approach to auditing

The use of a "process approach" is a requirement for all ISO management system standards in accordance with ISO/IEC Directives, Part 1, Annex SL. Auditors should understand that auditing a management system is auditing an organization's processes and their interactions in relation to one or more management system standard(s). Consistent and predictable results are achieved more effectively and efficiently when activities are understood and managed as interrelated processes that function as a coherent system.

A.3 Professional judgement

Auditors should apply professional judgement during the audit process and avoid concentrating on the specific requirements of each clause of the standard at the expense of achieving the intended outcome of the management system. Some ISO management system standard clauses do not readily lend themselves to audit in terms of comparison between a set of criteria and the content of a procedure or work instruction. In these situations, auditors should use their professional judgement to determine whether the intent of the clause has been met.

A.4 Performance results

Auditors should be focused on the intended result of the management system throughout the audit process. While processes and what they achieve are important, the result of the management system and its performance are what counts. It is also important to consider the level of the integration of different management systems and their intended results.

The absence of a process or documentation can be important in a high risk or complex organization but not so significant in other organizations.

A.5 Verifying information

Insofar as practicable, the auditors should consider whether the information provides sufficient objective evidence to demonstrate that requirements are being met, such as being:

a) complete (all expected content is contained in the documented information);

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

c) consistent (the documented information is consistent in itself and with related documents);

d) current (the content is up to date).

It should also be considered whether the information being verified provides sufficient objective evidence to demonstrate that requirements are being met.

If information is provided in a manner other than expected (e.g. by different individuals, alternate media), the integrity of the evidence should be assessed.

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).

A.6 Sampling

A.6.1 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 not be representative of the population from which they are selected. Thus, the auditor's conclusion may be biased and be different from 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:

a) establishing the objectives of sampling;

b) selecting the extent and composition of the population to be sampled;

c) selecting a sampling method;

d) determining the sample size to be taken;

e) conducting the sampling activity;

f) 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 A.6.2) or statistical sampling (see A.6.3).

A.6.2 Judgement-based sampling

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

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

a) previous audit experience within the audit scope;

b) complexity of requirements (including statutory and regulatory requirements) to achieve the audit objectives;

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

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

e) previously identified significant risks and opportunities for improvement;

f) 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.

A.6.3 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 conformity 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.

Elements that can affect the audit sampling plan are:

a) the context, size, nature and complexity of the organization;

b) the number of competent auditors;

c) the frequency of audits;

d) the time of individual audit;

e) any externally required confidence level;

f) the occurrence of undesirable and/or unexpected events.

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.

A.7 Auditing compliance within a management system

The audit team should consider if the auditee has effective processes for:

a) identifying its statutory and regulatory requirements and other requirements it is committed to;

b) managing its activities, products and services to achieve compliance with these requirements;

c) evaluating its compliance status.

In addition to the generic guidance given in this document, when assessing the processes that the auditee has implemented to ensure compliance with relevant requirements, the audit team should consider if the auditee:

1) has an effective process for identifying changes in compliance requirements and for considering them as part of the management of change;

2) has competent individuals to manage its compliance processes;

3) maintains and provides appropriate documented information on its compliance status as required by regulators or other interested parties;

4) includes compliance requirements in its internal audit programme;

5) addresses any instances of non-compliance;

6) considers compliance performance in its management reviews.

A.8 Auditing context

Many management systems standards require an organization to determine its context, including the needs and expectations of relevant interested parties and external and internal issues. To do this, an organization can use various techniques for strategic analysis and planning.

Auditors should confirm that suitable processes have been developed for this and are used effectively, so that their results provide a reliable basis for determining the scope and the development of the management system. To do this, auditors should consider objective evidence related to the following:

a) the process(es) or method(s) used;

b) the suitability and competence of the individuals contributing to the process(es);

c) the results of the process(es);

d) the application of the results to determine management system scope and development;

e) periodic reviews of context, as appropriate.

Auditors should have relevant sector-specific knowledge and understanding of the management tools that organizations can use in order to make a judgement regarding the effectiveness of the processes used to determine context.

A.9 Auditing leadership and commitment

Many management systems standards have increased requirements for top management.

These requirements include demonstrating commitment and leadership by taking accountability for the effectiveness of the management system and fulfilling a number of responsibilities. These include tasks that top management should undertake itself and others that can be delegated.

Auditors should obtain objective evidence of the degree to which top management is involved in decision-making related to the management system and how it demonstrates commitment to ensuring its effectiveness. This can be achieved by reviewing the results from relevant processes (for example policies, objectives, available resources, communications from top management) and by interviewing staff to determine the degree of top management engagement.

Auditors should also aim to interview top management to confirm that they have an adequate understanding of the discipline-specific issues relevant to their management system, together with the context their organization operates within, so that they can ensure that the management system achieves its intended results.

Auditors should not only focus on leadership at the top management level but should also audit leadership and commitment at other levels of management, as appropriate.

A.10 Auditing risks and opportunities

As part of the assignment of an individual audit the determination and management of the organization's risk and opportunities can be included. The core objectives for such an audit assignment are to:

— give assurance on the credibility of the risk and opportunity identification process(es);

— give assurance that risks and opportunities are correctly determined and managed;

— review how the organization addresses its determined risks and opportunities.

An audit of an organization's approach to the determination of risks and opportunities should not be performed as a stand-alone activity. It should be implicit during the entire audit of a management system, including when interviewing top management. An auditor should act in accordance with the following steps and collect objective evidence as follows:

a) inputs used by the organization for determining its risks and opportunities, which may include:

   — analysis of external and internal issues;

   — the strategic direction of the organization;

   — interested parties, related to its discipline-specific management system and their requirements, also;

   — potential sources of risk such as environmental aspects, and safety hazards, etc.

b) method by which risks and opportunities are evaluated, which can differ between disciplines and sectors.

The organization's treatment of its risk and opportunities, including the level of risk it wishes to accept and how it is controlled, will require the application of professional judgement by the auditor.

A.11 Life cycle

Some discipline-specific management systems require the application of a life cycle perspective to their products and services. Auditors should not consider this as a requirement to adopt a life cycle approach.

A life cycle perspective involves consideration of the control and influence the organization has over the stages of its product and service life cycle. Stages in a life cycle include acquisition of raw materials, design, production, transportation/delivery, use, end of life treatment and final disposal. This approach enables the organization to identify those areas where, in considering its scope, it can minimize its impact on the environment while adding value to the organization. The auditor should use their professional judgement as to how the organization has applied a life cycle perspective in terms of its strategy and the:

a) life of the product or service;

b) organization's influence on the supply chain;

c) length of the supply chain;

d) technological complexity of the product.

If an organization has combined several management systems into a single management system to meet its own needs, the auditor should look carefully at any overlap concerning consideration of the life cycle.

A.12 Audit of supply chain

The audit of the supply chain to specific requirements can be required. The supplier audit programme should be developed with applicable audit criteria for the type of suppliers and external providers. The scope of the supply chain audit can differ, e.g. complete management system audit, single process audit, product audit, configuration audit.

A.13 Preparing audit work documents

When preparing audit 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 audit 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.

A.14 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:

a) interviews with employees and other individuals;

b) observations of activities and the surrounding work environment and conditions;

c) documented information, such as policies, objectives, plans, procedures, standards, instructions, licences and permits, specifications, drawings, contracts and orders;

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

e) data summaries, analyses and performance indicators;

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

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

h) databases and websites;

i) simulation and modelling.

A.15 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 to auditors on security, health (e.g. quarantine), occupational health and safety matters and cultural norms and working hours 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;
- confirm the arrangements with the auditee regarding the use of mobile devices and cameras including recording information such as photographs of locations and equipment, screen shot copies or photocopies of documents, videos of activities and interviews, taking into consideration security and confidentiality matters;
- 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 (if applicable);
- ensure emergency procedures are communicated (e.g. emergency exits, assembly points);
- schedule communication to minimize disruption;

— adapt the 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 copies of documents in any media, 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.

c) Virtual audit activities:

— ensure that the audit team is using agreed remote access protocols including requested devices, software, etc.;

— if taking screen shot copies of document of any kind, ask for permission in advance and consider confidentiality and security matters and avoid recording individuals without their permission;

— if an incident occurs during the remote access, 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;

— use floor plans/diagrams of the remote location for reference;

— maintain respect for privacy during audit breaks.

Consideration needs to be given to disposition of information and audit evidence, irrespective of the type of media, at a later date, once the need for its retention has lapsed.

A.16 Auditing virtual activities and locations

Virtual audits are conducted when an organization performs work or provides a service using an on-line environment allowing persons irrespective of physical locations to execute processes (e.g. company intranet, a "computing cloud"). Auditing of a virtual location is sometimes referred to as virtual auditing. Remote audits refer to using technology to gather information, interview an auditee, etc. when "face-to-face" methods are not possible or desired.

A virtual audit follows the standard audit process while using technology to verify objective evidence. The auditee and audit team should ensure appropriate technology requirements for virtual audits which can include:

— ensuring the audit team is using agreed remote access protocols, including requested devices, software, etc.;

— conducting technical checks ahead of the audit to resolve technical issues;

— ensuring contingency plans are available and communicated (e.g. interruption of access, use of alternative technology), including provision for extra audit time if necessary.

Auditor competence should include:

— technical skills to use the appropriate electronic equipment and other technology while auditing;

— experience in facilitating meetings virtually to conduct the audit remotely.

When conducting the opening meeting or auditing virtually, the auditor should consider and the following items:

— risks associated with virtual or remote audits;

— using floor plans/diagrams of remote locations for reference or mapping of electronic information;

— facilitating for the prevention of background noise disruptions and interruptions;

— asking for permission in advance to take screen shot copies of documents or any kind of recordings, and considering confidentiality and security matters;

— ensuring confidentiality and privacy during audit breaks e.g. by muting microphones, pausing cameras.

A.17 Conducting interviews

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

a) interviews should be held with individuals from appropriate levels and functions performing activities or tasks within the audit scope;

b) interviews should normally be conducted during normal working hours and, where practical, at the normal workplace of the individual being interviewed;

c) attempts should be made to put the individual being interviewed at ease prior to and during the interview;

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

e) interviews may be initiated by asking individuals to describe their work;

f) the type of question used should be carefully selected (e.g. open, closed, leading questions, appreciative inquiry);

g) awareness of limited non-verbal communication in virtual settings; instead focus should be on the type of questions to use in finding objective evidence;

h) the results from the interview should be summarized and reviewed with the interviewed individual;

i) the interviewed individuals should be thanked for their participation and cooperation.

A.18 Audit findings

A.18.1 Determining audit findings

When determining audit findings, the following should be considered:

a) follow-up of previous audit records and conclusions;

b) requirements of the audit client;

c) accuracy, sufficiency and appropriateness of objective evidence to support audit findings;

d) extent to which planned audit activities are realized and planned results achieved;

e) findings exceeding normal practice, or opportunities for improvement;

f) sample size;

g) categorization (if any) of the audit findings.

A.18.2Recording conformities

For records of conformity, the following should be considered:

a) description of or reference to audit criteria against which conformity is shown;

b) audit evidence to support conformity and effectiveness, if applicable;

c) declaration of conformity, if applicable.

A.18.3Recording nonconformities

For records of nonconformity, the following should be considered:

a) description of or reference to audit criteria;

b) audit evidence;

c) declaration of nonconformity;

d) related audit findings, if applicable.

A.18.4Dealing 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:

a) separate findings for each criterion; or

b) 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 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[2] ISO 9001, *Quality management systems — Requirements*[1]

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

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

[1] See www.iso.org/tc176/ISO9001AuditingPracticesGroup.