Guidelines for auditing management systems

Lignes directrices pour l’audit des systèmes de management

[Revision of first edition (ISO 19011:2002)]

ICS 03.120.10; 13.020.10
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>v</td>
</tr>
<tr>
<td>Introduction</td>
<td>vi</td>
</tr>
<tr>
<td>1 Scope</td>
<td>1</td>
</tr>
<tr>
<td>2 Normative references</td>
<td>1</td>
</tr>
<tr>
<td>3 Terms and definitions</td>
<td>1</td>
</tr>
<tr>
<td>4 Principles of auditing</td>
<td>3</td>
</tr>
<tr>
<td>5 Managing an audit programme</td>
<td>5</td>
</tr>
<tr>
<td>5.1 General</td>
<td>5</td>
</tr>
<tr>
<td>5.2 Establishing the audit programme</td>
<td>6</td>
</tr>
<tr>
<td>5.2.1 Developing the programme objectives</td>
<td>6</td>
</tr>
<tr>
<td>5.2.2 Role and responsibility of the person(s) managing audit programme(s)</td>
<td>7</td>
</tr>
<tr>
<td>5.2.3 Competence of the person responsible for managing audit programme(s)</td>
<td>7</td>
</tr>
<tr>
<td>5.2.4 Determining the extent of an audit programme</td>
<td>8</td>
</tr>
<tr>
<td>5.2.5 Evaluating audit programme risks</td>
<td>8</td>
</tr>
<tr>
<td>5.2.6 Establishing audit programme procedures</td>
<td>9</td>
</tr>
<tr>
<td>5.2.7 Identifying audit programme resources</td>
<td>9</td>
</tr>
<tr>
<td>5.3 Implementing the audit programme</td>
<td>9</td>
</tr>
<tr>
<td>5.3.1 General</td>
<td>9</td>
</tr>
<tr>
<td>5.3.2 Defining individual audit objectives, scope and criteria</td>
<td>10</td>
</tr>
<tr>
<td>5.3.3 Determining the audit method(s)</td>
<td>10</td>
</tr>
<tr>
<td>5.3.4 Selecting the audit team</td>
<td>11</td>
</tr>
<tr>
<td>5.3.5 Assigning responsibility for individual audit(s) to the audit team leader</td>
<td>12</td>
</tr>
<tr>
<td>5.3.6 Managing and maintaining audit programme records</td>
<td>12</td>
</tr>
<tr>
<td>5.4 Audit programme monitoring</td>
<td>13</td>
</tr>
<tr>
<td>5.5 Reviewing and improving audit programmes</td>
<td>14</td>
</tr>
<tr>
<td>6 Audit activities</td>
<td>14</td>
</tr>
<tr>
<td>6.1 General</td>
<td>14</td>
</tr>
<tr>
<td>6.2 Initiating the audit</td>
<td>15</td>
</tr>
<tr>
<td>6.2.1 General</td>
<td>15</td>
</tr>
<tr>
<td>6.2.2 Establishing initial contact with the auditee</td>
<td>15</td>
</tr>
<tr>
<td>6.2.3 Determining the feasibility of the audit</td>
<td>16</td>
</tr>
<tr>
<td>6.3 Preparing for the audit activities</td>
<td>16</td>
</tr>
<tr>
<td>6.3.1 Preparing the audit plan</td>
<td>16</td>
</tr>
<tr>
<td>6.3.2 Assigning work to the audit team</td>
<td>17</td>
</tr>
<tr>
<td>6.3.3 Preparing work documents</td>
<td>17</td>
</tr>
<tr>
<td>6.4 Conducting audit activities</td>
<td>18</td>
</tr>
<tr>
<td>6.4.1 Document review</td>
<td>18</td>
</tr>
<tr>
<td>6.4.2 Conducting opening meeting</td>
<td>18</td>
</tr>
<tr>
<td>6.4.3 Communication during the audit</td>
<td>19</td>
</tr>
<tr>
<td>6.4.4 Roles and responsibilities of guides and observers</td>
<td>19</td>
</tr>
<tr>
<td>6.4.5 Collection and verification of information</td>
<td>20</td>
</tr>
<tr>
<td>6.4.6 Audit findings</td>
<td>21</td>
</tr>
<tr>
<td>6.5 Conducting the audit</td>
<td>22</td>
</tr>
<tr>
<td>6.5.1 Preparing the audit report</td>
<td>23</td>
</tr>
<tr>
<td>6.5.2 Distributing the audit report</td>
<td>23</td>
</tr>
<tr>
<td>6.6 Completing the audit</td>
<td>24</td>
</tr>
<tr>
<td>6.7 Conducting audit follow-up</td>
<td>24</td>
</tr>
</tbody>
</table>
7 Competence and evaluation of auditors .................................................................25
  7.1 General .............................................................................................................25
  7.2 Determine auditor competence to meet the needs of the audit programme .......25
  7.2.1 Personal behaviours .....................................................................................26
  7.2.2 Knowledge and skills ..................................................................................26
  7.2.3 Education, work experience, training and audit experience of auditors .......29
  7.3 Establish the evaluation criteria ......................................................................29
  7.4 Select the appropriate evaluation method .......................................................29
  7.5 Conduct the evaluation ...................................................................................30
  7.6 Maintenance and improvement of competence ..............................................30

Annex A (Informative) Discipline-specific knowledge and skills of auditors ..........32
  A.1 General ...........................................................................................................32
  A.2 Discipline-specific knowledge and skills of auditors – Quality .......................32
  A.3 Discipline-specific knowledge and skills of auditors – Environmental ............33
  A.4 Discipline-specific knowledge and/or skills of auditors – Occupational health and safety (OH&S) .................................................................35
  A.5 The discipline-specific knowledge and/or skills of auditors – Resilience, security, preparedness and continuity (RSPC) management ......................36
  A.6 The discipline-specific knowledge and/or skills of auditors - Discipline: Transportation safety management.................................................................38
  A.7 Discipline-specific knowledge and skills of auditors – Records .......................39

Annex B (Informative) Examples of discipline specific evaluations of audit team competence ........42
  B.1 General ...........................................................................................................42
  B.2 Application of the evaluation process for an audit team undertaking an internal audit of an aviation organization’s quality and environmental management systems .................43
  B.3 Application of the evaluation process for an audit team undertaking an internal audit of an event management organization’s Quality and OH&S management systems ...........................................49
  B.4 Application of the evaluation process for an auditor in a hypothetical resilience, security, preparedness and/or continuity management internal audit programme .........................................................52

Annex C (Informative) Additional Guidance for Auditors for Planning and Conducting Audits ......61
  C.1 Applying audit methods ..................................................................................61
  C.2 Sources of information ...................................................................................62
  C.3 Conducting document review ........................................................................62
  C.4 Preparing Work Documents ........................................................................63
  C.5 Sampling strategy considerations for audits ...................................................63
  C.6 Guidance for site visits and observations .......................................................65
  C.7 Conducting interviews ...................................................................................66
  C.8 Audit findings ................................................................................................66

Bibliography ........................................................................................................68
Foreword

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

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

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

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

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

ISO 19011:2011 was prepared under the auspices of the Joint Technical Coordination Group and administered by Technical Committee ISO/TC 176, Quality management and quality assurance, Subcommittee SC 3, Supporting technologies. Members of Working Group 16 under TC 176/SC 3 included representatives of other technical committees (e.g., TC 207, TC 34) and other interested parties for the management systems included within the scope of this standard.

This second edition of ISO 19011 cancels and replaces ISO 19011: 2002 which has been technically revised.
Introduction

Since the initial publication of ISO 19011 in 2002, a number of new management system standards have been published. This has resulted in a need to consider a broader scope of management system auditing as well as provide guidance that is more generic.

In 2006, ISO CASCO developed a standard with requirements for 3rd party management system certification audit purposes in ISO/IEC 17021.

It is in this context that this revision of ISO 19011 provides guidance for all users, including small and medium sized enterprises, specially concentrating on what are commonly termed internal (first party) and second party audit.

This International Standard does not state requirements but provides guidance on the management of audit programmes and on the conduct of audits of management systems, as well as on the competence and evaluation of auditors and audit teams. Users of this International Standard may, however, apply this guidance in developing their own audit-related requirements.

This guidance is intended to apply to a broad range of potential users, including auditors, organizations implementing management systems, and organizations needing to conduct audits of management systems for contractual or regulatory reasons. It may also be used for the purpose self-declaration. It may also be useful to organizations involved in auditor training or certification.

The guidance in this International Standard is intended to be flexible. As indicated at various points in the text, the use of this guidance may differ according to the size, level of maturity of an organizations’ 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.

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

Clause 5 provides guidance on the establishment and management of audit programmes, including establishing the audit programme objectives, and coordinating auditing activities.

Clause 6 provides guidance on conducting audits of management systems.

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

Annex A illustrates the application of the guidance in Clause 7 to different disciplines (e.g. quality, environmental, occupational health and safety, resilience, security, preparedness and continuity management and transportation safety management).

Annex B provides examples of the evaluation of audit team competencies in various hypothetical organizations in different sectors (e.g. aviation, event management).

Annex C provides additional guidance for auditors on planning and conducting audits.
Guidelines for auditing management systems

1 Scope

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

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

The application of this International Standard to other types of audit is possible, provided that special consideration is paid to the specific competences needed.

2 Normative references

Where standards or other documents have been used or referred to (e.g. for some definitions in clause 3) it was decided to include the original text in the present International standard in order to create a stand-alone document.

A bibliography at the end of this present International standard lists these documents as well as other useful source material.

3 Terms and definitions

For the purposes of this document, the following terms and definitions given below apply. All efforts have been taken that these definitions should not conflict with the definitions used in other management system standards.

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

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

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

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

NOTE 4 When two or more auditing organizations cooperate to audit a single auditee (3.7), this is termed a joint audit.
3.2 **audit criteria**
set of policies, procedures or requirements

NOTE 1 Audit criteria are used as a reference against which **audit evidence** (3.3) is compared.

NOTE 2 If the audit criteria are selected from legal or other requirements, the audit finding (3.4) is termed compliance or non-compliance.

NOTE 3 If the audit criteria are selected from standards (internal or external), the audit finding (3.4) is termed a **conformity** (3.16) or **nonconformity** (3.17).

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

NOTE Audit evidence may be qualitative or quantitative.

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

NOTE Audit findings may indicate **conformity** (3.16), **nonconformity** (3.17), and opportunities for improvement or good practices.

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

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

NOTE The audit client may be the **auditee** (3.7) or any other organization which has the regulatory or contractual right to request an audit.

3.7 **auditee**
organization being audited

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

3.9 **audit team**
one or more **auditors** (3.8) conducting an **audit** (3.1), supported if needed by **technical experts** (3.15)

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

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

3.10 **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

3.11 **audit plan**
description of the activities and arrangements for an **audit** (3.1)
3.12 risk

3.13 audit scope

extent and boundaries of an audit (3.1)

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

3.14 competence

ability to apply knowledge and skills to achieve intended results.

NOTE ability implies the appropriate application of personal behaviour during the audit process

3.15 technical expert

person who provides specific knowledge or expertise to the audit team (3.9)

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

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

3.16 conformity

fulfilment of a requirement

3.17 nonconformity

non-fulfilment of a requirement

3.18 guide

person appointed by the auditee to assist the audit team

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 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 following principles relate to auditors and those who manage the audit programme(s).

a) Integrity: the foundation of professionalism

Auditors and those who manage the audit programme(s) should:
perform their work with honesty, diligence, and responsibility;

observe and respect any applicable legal requirements;

demonstrate their technical competence while undertaking their work;

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

be sensitive to any influences that may be exerted by other interested parties on their judgment 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 may be reported. The communication has to 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 be prudent in the use and protection of information acquired in the course of their duties. Audit information should not be used inappropriately for the personal gain by the auditor or the audit client or in a manner detrimental to the legitimate interest of the auditee. This concept includes the proper handling of sensitive, confidential or classified information.

The following two principles relate to the audit, which is by definition an independent and systematic activity.

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 and act in a manner that is free from bias and conflict of interest wherever possible. For internal audits, auditors should be independent from the operating managers of the function(s) being audited. Auditors should maintain an objective state of mind 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 allow for objectivity.

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

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

The guidance given in the remaining clauses of this International Standard is based on the principles set out above.
5 Managing an audit programme

5.1 General

An organization needing to conduct audits should establish an audit programme(s). The audit client should set the objective(s) to be achieved by the audit programme(s). The programme(s) should be able to determine the effectiveness of the auditee’s management system in meeting its objectives.

The audit client should assign (a) competent person(s) with responsibility for managing the audit programme(s).

The programme should be adequately and effectively established and implemented. The audit programme should include planning the types and number of audits needed, as well as providing information and resources necessary to organize and conduct its audits effectively and efficiently within the specified time frames.

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 and the level of maturity of the management system to be audited. Priority should be given to allocating the audit programme resources to audit those matters of significance within the management system. These may include the key characteristics of product or service quality, safety and health hazards and risks and significant environmental aspects and their control.

NOTE This concept is commonly known as risk-based auditing.

The audit programme(s) can include audits of single, multiple or integrated management system(s) conducted either separately or in combination.

The results monitored and measured to ensure the objective has been achieved. The audit programme should be reviewed in order to identify the possible improvements.

The audit programme should include:

- the audit objectives;
- extent/number/types/locations/schedule of the audits;
- main audit procedure;
- audit criteria;
- audit methods;
- selection of audit team(s);
- uncertainty in achieving objectives of the audit programme and preventive measures to be implemented;
- necessary resources, including travel and accommodations;
- processes for handling confidentiality, information security and other similar matters;
Figure 1 — Illustration of the flow for the management of an audit programme

NOTE 1 Figure 1 also illustrates the application of the Plan-Do-Check-Act methodology in this International Standard.

NOTE 2 The numbers in this and all subsequent figures refer to the relevant clauses of this International Standard.

5.2 Establishing the audit programme

5.2.1 Developing the programme objectives

Objectives for an audit programme(s), to direct the planning and conduct of audits and to ensure the audit programme is implemented effectively.

These objectives can vary depending on:

— management priorities;
— commercial and/or business intentions;
— management system(s) requirements;
— legal and other requirements;
— need for supplier evaluation;
— needs and expectations of interested parties (including customers);
— auditee’s level of performance, as reflected in the occurrence of failures or incidents or customer complaints;
Examples of audit programme objectives may include the following:

- to contribute to the improvement of a management system and its performance;
- to meet external requirements, e.g. certification to a management system standard;
- to verify conformity with contractual requirements;
- to obtain and maintain confidence in the capability of a supplier;
- to evaluate compatibility and alignment of the management system objectives with the management system policy and the overall business objectives;

5.2.2 Role and responsibility of the person(s) managing audit programme(s)

The person(s) assigned the responsibility for managing the audit programme(s) should:

- establish the extent of the audit programme;
- evaluate the risks for the audit programme;
- establish audit responsibilities and procedures;
- ensure necessary resources are provided, including the evaluation of auditors;
- ensure the implementation of the audit programme, such as defining audit objectives, scope and criteria of the individual audits, determining audit methods and selecting the audit team;
- ensure that appropriate audit programme records are managed and maintained;
- monitor, review and improve the audit programme.

The person(s) assigned the responsibility for managing an audit programme(s) should inform the top management on the contents of the audit programme and, where necessary, ask for its approval.

5.2.3 Competence of the person responsible for managing audit programme(s)

The person(s) responsible for managing the audit programme(s) should have competence to manage the audit programme(s) effectively and efficiently as well as competence in the following areas relevant to their organization and the audit programme objectives:

- audit principles, procedures, methods and techniques;
- management system and reference documents;
- applicable legal and other requirements relevant to the activities and/or products of the organization to be audited;
- organizational product and processes;
- customer(s), supplier(s) and other interested parties of the organization to be audited, where applicable;
5.2.4 Determining the extent of an audit programme

The person(s) responsible for managing audit programme(s) should establish the extent of an audit programme which can vary depending on the size and nature of the organization to be audited, as well as on the nature, functionality, complexity and the level of maturity of the management system(s) to be audited. Other factors impacting the extent of an audit programme include:

- the scope, objective and duration of each audit to be conducted;
- the frequency of the audits to be conducted;
- the number, importance, similarity and locations of the activities to be audited;
- those matters of significance to the effectiveness of the management system;
- legal and other requirements, such as standards, contractual requirements and other audit criteria;
- the need to meet external requirements, e.g. for certification;
- conclusions of previous internal or external audits or results of a previous audit programme review;
- language, cultural and social issues;
- the concerns of interested parties, such as customer complaints or regulatory breaches;
- significant changes to the organization to be audited or its operations;
- the extent and maturity of the information and communications technologies of the auditee, which can impact the use of remote audit methods;
- the occurrence of internal and external events such as product failure, contamination, information security leak, health and safety incident, criminal acts or environmental incident.

5.2.5 Evaluating audit programme risks

There are a variety of risks associated with establishing, implementing, monitoring and reviewing an audit programme that may affect the audit programme objectives. The person(s) responsible for managing the audit programme should consider these risks when developing an audit programme. These risks may be associated with:

- planning, e.g. failure to set relevant audit objectives and determine the extent of the audit programme;
- resources, e.g. allowing insufficient time for the person responsible for managing the audit programme to develop the audit programme;
- selection of the audit team, e.g. the team does not have the collective competence to conduct the audit effectively;
- implementation, e.g. ineffective communication of the audit programme;
- records, e.g. failure to adequately protect audit records to demonstrate audit programme effectiveness;
- monitoring, reviewing and improving the audit programme, e.g. ineffective monitoring of audit programme outcomes.
5.2.6 Establishing audit programme procedures

The person(s) responsible for managing audit programme(s) should establish one or more audit programme procedures, addressing the following:

- planning and scheduling audits considering audit programme risks;
- managing information security, confidentiality, risks to the organization from auditing activities and other matters related to the audit programme;
- assuring the competence of auditors and audit team leaders;
- selecting appropriate audit teams and assigning their roles and responsibilities;
- conducting audits, including the use of appropriate sampling methods;
- conducting audit follow-up, if applicable;
- reporting to the audit client (e.g. top management) on the overall achievements of the audit programme;
- maintaining audit programme records;
- monitoring the performance, risks and effectiveness of the audit programme.

5.2.7 Identifying audit programme resources

When identifying resources for the audit programme, the person(s) responsible for managing audit program(s) should consider:

- the financial resources necessary to develop, implement, manage and improve audit activities;
- audit methods/techniques;
- the availability of auditors and technical experts having competence appropriate to the particular audit programme objectives;
- the extent of the audit programme;
- travelling time and cost, accommodation and other auditing needs;
- the extent and maturity of the information and communication systems of the organization to be audited which may impact the use of remote audit methods.

5.3 Implementing the audit programme

5.3.1 General

The person(s) responsible for managing audit programme(s) should implement the audit programme by:

- communicating the pertinent parts of the audit programme to relevant parties and informing them periodically of its progress;
- defining objectives, scope and criteria for each individual audit;
- coordinating and scheduling audits and other activities relevant to the audit programme;
- ensuring the selection of audit teams with the necessary competence;
5.3.2 Defining individual audit objectives, scope and criteria

Based on the information contained in the audit programme and in order to develop the audit plan for each individual audit, it is necessary to identify and document the specific audit objectives, scope, methods, criteria and procedures.

The audit objectives define what is to be accomplished by the individual audit and should be documented in the audit plan. They may include the following:

- determination of the extent of conformity of a management system to be audited, or parts of it, with audit criteria;
- evaluation of the capability of a management system to ensure compliance with legal and other requirements;
- evaluation of the effectiveness of a management system in meeting its specified objectives;
- identification of areas for potential improvement of a management system;
- treatment of confidential information including the extent of disclosure.

The individual audit objectives should be defined by the person responsible for managing the audit programme and be consistent with the overall audit programme objectives.

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

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

The audit scope and audit criteria should be defined jointly by the person(s) responsible for managing audit programme and the audit team leader in accordance with audit programme procedures. Any changes to the audit objectives, audit scope or audit criteria should be agreed to by the same parties and the audit programme should be modified accordingly.

Where a combined audit is to be conducted, it should be ensured that the:

- audit objectives arising from different audit programmes are aligned, including those objectives arising from the combination;
- audit scope is consistent with requirements arising from the specific management system standards;
- audit criteria are selected so that efficiency can be gained by combining similar requirements/subjects from different references.

5.3.3 Determining the audit method(s)

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

NOTE Guidance how to determine audit methods is given in Annex C
Where two or more auditing organizations conduct a joint audit in the same auditee, the persons responsible for the management of the different audit programmes should cooperate and exchange information during the establishment of the audit programmes. They should pay special attention to the division of responsibilities, the scheduling of the joint audits, the provision of any additional resources, the competence of the audit team and the appropriate procedures. Agreement on these matters should be reached before the audit activities start.

If an organization to be audited operates two or more management systems of different disciplines, combined audits may be included in the audit programme. In such a case, special attention should be paid to the competence of the audit team.

### 5.3.4 Selecting the audit team

The person(s) responsible for managing audit programme(s) should appoint the members of the audit team, including the team leader and any technical expert(s) 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 processes for evaluating auditors.

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

- the overall competence of the audit team needed to achieve audit objectives, scope and criteria;
- whether the audit is a combined or joint audit;
- the kind of audit methods that have been selected;
- legal and other requirements such as contractual requirements;
- the need to ensure the independence of the audit team from the activities to be audited and to avoid any conflict of interest;
- the ability of the audit team members to interact effectively with the representatives of the auditee and to work together;
- the language of the audit, and an understanding of the auditee’s particular social and cultural characteristics. These issues may be addressed either by the auditor's own skills or through the support of a technical expert.

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

- identification of the knowledge and skills needed to achieve the objectives of the audit;
- selection of the audit team members so that all of the necessary knowledge and skills are present in the audit team.

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

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

Both the audit client and the auditee may request the replacement of particular audit team members on reasonable grounds based on the principles of auditing described in clause 4. Examples of reasonable grounds include conflict of interest situations (such as in the case of second or third party audits, an audit team member having been a...
former employee of the auditee or having provided consultancy services to the auditee), lack of competency or previous unethical behaviour. Such grounds should be communicated to the audit team leader and to the person assigned responsibility for managing the audit programme, who should discuss the issue with the audit client and auditee before making any decisions or replacing audit team members.

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.

5.3.5 Assigning responsibility for individual audit(s) to the audit team leader

The person responsible for the management of the audit programme should assign the responsibility for the conduct of the individual audit to an audit team leader. The assignment should be made in sufficient time to ensure the effective planning of the audits.

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

— the audit objectives;
— the audit criteria and any reference documents;
— the audit methods and procedures;
— the audit scope, including identification of the organizational and functional units and processes to be audited;
— the composition of the audit team;
— the locations (sites), dates, and duration of the audit activities to be conducted;
— the allocation of appropriate resources to conduct the audit.

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

— the working and reporting language of the audit where this is different from the language of the auditor and/or the auditee;
— audit report contents requested by the audit programme;
— matters related to confidentiality and information security, if required by the audit programme;
— any follow-up actions, for example, from a previous audit, if applicable;
— coordination with other audit activities, in case of a joint audit.

The person responsible for the audit programme should ensure that the information provided adequately addresses identified risks to the achievement of audit objectives.

5.3.6 Managing and maintaining audit programme records

The person(s) responsible for managing audit programme(s) should manage and maintain records to demonstrate the implementation of the audit programme. Processes should be established to ensure that any privacy or confidentiality needs associated with the audit records are satisfied.

Records should include the following:

a) Records related to the audit programme such as;
582  — audit programme objectives;
583  — those addressing audit programme risks;
584  — reviews of the audit programme effectiveness.
585  b) records related to individual audit, such as
586  — audit plans and audit reports;
587  — nonconformity reports;
588  — corrective and preventive action reports;
589  — audit follow-up reports, if applicable.
590  c) records related to audit personnel covering subjects such as
591  — competence and performance evaluation of the audit team members;
592  — audit team selection;
593  — maintenance and improvement of competence.
594  The form and level of details of the records should meet the objectives of the audit programme(s).

5.4 Audit programme monitoring

596  The person(s) responsible for managing audit program(s) should monitor the implementation of the audit programme(s) at periodic intervals considering the need to;
597  — review and approve audit reports, and ensure their distribution to the top management and other relevant parties.
598  — determine the necessity of any follow-up audit;
599  — evaluate the performance of the audit team members;
600  — evaluate the ability of the audit teams to implement the audit plan;
601  — evaluate conformity with audit programmes, schedules and audit objectives;
602  — evaluate feedback from top management, auditees, auditors and other interested parties.
603  Some factors may determine the need to modify the audit programme, before its completion, such as:
604  — initial audit findings;
605  — demonstrated level of management system effectiveness;
606  — changes to the client’s or the auditee’s management system;
607  — change of legal requirements and/or standard;
608  — change of supplier.
5.5 Reviewing and improving audit programmes

The person(s) responsible for managing audit programme(s) should review the audit programme to assess whether its objectives have been met. Lessons learned from the audit programme review should be used for the continual improvement process.

The audit programme review should consider, for example:

- results and trends from monitoring;
- conformity with audit programme procedure(s);
- evolving needs and expectations of interested parties;
- audit programme records;
- alternative or new auditing methods;
- effectiveness of the measures to address risks associated with audit programme;
- confidentiality and information security issues relating to the audit programme.

The person(s) responsible for managing audit programme(s) should review the overall implementation of audit programme(s), identify the area of improvement and amend the programme if necessary. They should also:

- review the continual professional development of auditors, in accordance with 7.4, 7.5 and 7.6;
- report the results of the audit programme review to the top management.

6 Audit activities

6.1 General

This clause contains guidance on planning and conducting audit activities using different audit methods as part of an audit programme. Figure 2 provides an overview of typical audit activities. The extent to which the provisions of this clause are applicable depends on the scope and complexity of the specific audit and the intended use of the audit conclusions.
6.2 Initiating the audit

6.2.1 General

6.2.2 Establishing initial contact with the auditee

6.2.2 Determining the feasibility of the audit

6.3 Preparing for the audit activities

6.3.1 Preparing the audit plan

6.3.2 Assigning work to the audit team

6.3.3 Preparing work documents

6.4 Conducting audit activities

6.4.1 Document review

6.4.2 Conducting the opening meeting

6.4.3 Communication during the audit

6.4.4 Roles and responsibilities of guides and observers

6.4.5 Collection and verification of information

6.4.6 Audit findings

6.4.7 Audit conclusions

6.4.8 Conducting the closing meeting

6.5 Preparing and distributing the audit report

6.5.1 Preparing the audit report

6.5.2 Distributing the audit report

6.6 Completing the audit

6.7 Conducting audit follow-up (if applicable)

Figure 2 — Overview of typical activities during an audit

6.2 Initiating the audit

6.2.1 General

When an audit is initiated, the responsibility for this audit is assigned to the audit team leader, as is defined in the audit programme. This assignment is performed by the person who is responsible for managing the audit programme by transferring information for the audit (see 5.3.5).

The responsibility for conducting the assigned audit remains with the audit team leader until the audit is completed.

To initiate an audit, the following steps should be considered, however the sequence can differ depending on the auditee, processes and specific situations.

6.2.2 Establishing initial contact with the auditee

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

— to establish communication channels with the auditee’s representative(s);

— to confirm the authority to conduct the audit;

— to provide information on the audit scope, audit methods and audit team composition;
---
650 — to request access to relevant documents for planning purposes, including records;
651 — to determine applicable legal and other requirements;
652 — to confirm the agreement with the auditee regarding the extent of the disclosure and the treatment of the
653 confidential information;
654 — to make arrangements for the audit including scheduling the date(s);
655 — to agree on the attendance of observers and the need for guides for the audit team;
656 — to find out, the expectations and needs the auditee has related to the specific audit.

6.2.3 Determining the feasibility of the audit

The feasibility of an audit determines whether all of the necessary resources, information, arrangements, etc., are
in place to provide reasonable confidence that the audit objectives can be achieved.

The feasibility of the audit should be determined, taking into consideration such factors as the availability of:

651 — sufficient and appropriate information for planning the audit;
652 — adequate cooperation from the auditee; and
653 — adequate time and resources for performing the audit.

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

6.3 Preparing for the audit activities

6.3.1 Preparing the audit plan

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

The amount of detail provided in the audit plan should reflect the scope and complexity of the audit as well as risks
and the effect of uncertainty on the audit outcome. In preparing the audit plan the audit team leader should be
aware of appropriate sampling techniques (see Annex C.5), compatibility of audit team members and risks to the
organization created by the audit.

NOTE  Risks to the organization may include an audit team member who mishandle the auditee’s information, creates a
safety, health, environmental or a security risk such as a threat to the auditee’s products, services, personnel and/or
infrastructure.

For combined and joint audits, particular attention should be given to the interfaces between processes of the
management system(s).

681 The details may differ, for example, between initial and subsequent audits and also between internal and external
audits. The audit plan should be sufficiently flexible to permit changes which can become necessary as the audit
activities progress.

684 The audit plan should cover or reference the following:

685 — the audit objectives;
686 — the audit scope, including identification of the organizational and functional units and processes to be audited;
687 — the audit criteria and any reference documents;
688 — the locations, dates, expected times and duration of audit activities to be conducted, including meetings with
689 the auditee’s management as well as other meetings;
690 — the audit method to be used including the extent to which audit sampling is needed to obtain sufficient audit
691 evidence and the design of the sampling programme, if applicable;
692 — the roles and responsibilities of the audit team members as well as guides and observers;
693 — the allocation of appropriate resources to critical areas of the audit.
694 The audit plan should also cover the following, as appropriate:
695 — identification of the auditee’s representative for the audit;
696 — the working and reporting language of the audit where this is different from the language of the auditor and/or
697 the auditee;
698 — the audit report topics;
699 — logistics and communications arrangements including specific arrangements for the sites to be audited;
700 — any specific measures taken to address risks and the effect of uncertainty on the audit objectives;
701 — matters related to confidentiality and information security;
702 — any follow-up actions, for example, from a previous audit;
703 — co-ordination with other audit activities, in case of a joint audit.
704 The plan should be reviewed and accepted by the audit client, and presented to the auditee, before the audit
705 activities begin.
706 Any objections by the auditee should be resolved between the audit team leader, the auditee and/or the person
707 responsible for managing the audit programme. Any revised audit plan should be agreed among the parties
708 concerned before continuing the audit.

6.3.2 Assigning work to the audit team

709 The audit team leader, in consultation with the audit team, should assign to each team member responsibility for
710 auditing specific processes, functions, sites, areas or activities. Such assignments should respect the
711 independence and competence of auditors and the effective use of resources, as well as different roles and
712 responsibilities of auditors, auditors-in-training and technical experts.
713 Audit team briefings, which should be held on a regular basis by the audit team leader, should allocate work
714 assignments and decide possible changes. Changes to the work assignments can be made as the audit
715 progresses to ensure the achievement of the audit objectives.

6.3.3 Preparing work documents

716 The audit team members should review the information relevant to their audit assignments and prepare work
717 documents as necessary for reference and for recording audit evidences. Such work documents should include:
720 — checklists and audit sampling plans;
forms for recording information, such as supporting evidence, audit findings and records of meetings.

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

NOTE Guidance on preparing work documents is given in Annex C.4 of this standard.

Work documents, including records resulting from their use, should be retained at least until audit completion. Retention of documents after audit completion is described in 6.7. Those documents 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 Document review

As a part of the audit activities the relevant auditee management system documentation should be reviewed to:

- gather information for the preparation of the audit activities;
- get an overview on the extent of the system documentation;
- determine the conformity of the system, as far as documented, with audit criteria.

NOTE Guidance how to perform a document review is provided in Annex C.3 of this standard.

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

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

If adequate documentation cannot be provided within the time frame given in the audit plan, the audit team leader should inform the person responsible for managing the audit programme, and the auditee. Depending on the audit scope and objectives a decision should be made as to whether the audit should be continued or suspended until documentation concerns are resolved.

#### 6.4.2 Conducting opening meeting

The purpose of the opening meeting is to confirm the audit plan, introduce the audit team and ensure that all planned audit activities are in place.

An opening meeting should be held with the auditee management and, where appropriate, those responsible for the functions or processes to be audited.

In many instances, for example 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 the attendance should be kept. The meeting should be chaired by the audit team leader, and the following items should be considered, as appropriate:

- introduction of the participants including observers and guides, and an outline of their roles;
- confirmation of the audit objectives, scope and criteria;
- confirmation of the audit plan and other relevant arrangements with the auditee, such as the date and time for the closing meeting, any interim meetings between the audit team and the auditee’s management, and any late changes;
⎯ presentation of the methods to be used to conduct the audit, including advising the auditee that the audit evidence will be based on a sample of the information available;

⎯ introduction of methods to manage risks to the organization, products, services, personnel and/or infrastructure associated with the audit;

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

⎯ confirmation of the language(s) to be used during the audit;

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

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

⎯ confirmation of matters relating to confidentiality and information security;

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

⎯ information on method of reporting audit findings including any grading;

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

⎯ information about the closing meeting;

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

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

6.4.3 Communication during the audit

It may be necessary to make formal arrangements for communication within the audit team with the auditee and potentially with external bodies (e.g. regulators) during the audit, especially where legislative requirements require the mandatory reporting of nonconformities.

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

During the audit, the audit team leader should periodically communicate the progress of the audit and any concerns to the auditee and audit client, as appropriate. Evidence collected during the audit that suggests an immediate and significant risk to the auditee should be reported without delay to the auditee and, as appropriate, to the audit client.

Any concern about an issue outside the audit scope should be noted and reported to the audit team leader, for possible communication to the audit client and auditee.

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

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

6.4.4 Roles and responsibilities of guides and observers

Guides and observers (e.g. regulator or other interested parties) may accompany the audit team. They should not influence or interfere with the conduct of the audit.
Guides, appointed by the auditee, should assist the audit team and act on the request of the audit team leader. Their responsibilities should include the following:

- establishing contacts and timing for interviews;
- arranging access to specific parts or sites of the auditee;
- ensuring that rules concerning site safety and security procedures are known and respected by the audit team members and observers;
- witnessing the audit on behalf of the auditee;
- providing clarification or assisting in collecting information.

### 6.4.5 Collection and verification of information

During the audit, information relevant to the audit objectives, audit scope and audit criteria, including information relating to interfaces between functions, activities and processes, should be collected by means of appropriate sampling and should be verified. Only information that is verifiable should be accepted as audit evidence. Audit evidence relevant to the audit findings should be recorded. If during collection of evidences, the audit team becomes aware of any new or changed risk, they should be addressed accordingly.

**NOTE** Guidance on sampling is given in Annex C.5 of this standard.

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

- interviews;
- observations;
- review of documents.

**NOTE 1** Guidance on sources of information is given in Annex C.1 of this standard.

**NOTE 2** Guidance on site-visits is given in Annex C.6 of this standard.

**NOTE 3** Guidance how to conduct interviews is given in Annex C.7 of this standard.

**6.4.6 Audit findings**

Audit evidence should be evaluated against the audit criteria to identify the audit findings. Audit findings can indicate conformity or nonconformity with audit criteria. When specified by the audit objectives, audit findings should identify opportunities for improvement and provide recommendations for best practice, where this does not compromise independence.

The audit team should meet as needed to review the audit findings at appropriate stages during the audit.
Conformity with audit criteria should be summarized to indicate locations, functions or processes that were audited.

If included in the audit plan, individual audit findings of conformity and their supporting evidence should also be recorded.

Nonconformities and their supporting audit evidence should be recorded. Nonconformities may be graded. They should be reviewed with the auditee 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 and/or findings, and unresolved points should be recorded.

For combined and joint audits, arrangements on dealing with findings related to criteria coming from the different requirements audited (multiple criteria) should be in place.

NOTE Additional guidance on identifying and evaluating of audit findings is given in Annex C.8 of this standard.

6.4.7 Audit conclusions

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

- review the audit findings, and any other appropriate information collected during the audit, against the audit objectives;
- agree on the audit conclusions, taking into account the uncertainty inherent in the audit process;
- prepare recommendations, if specified by the audit objectives;
- discuss audit follow-up, as applicable.

Audit conclusions can address issues such as:

- the extent of conformity of the management system with the audit criteria, including the effectiveness of the management system in meeting the stated objectives;
- the effective implementation, maintenance and improvement of a management system;
- the capability of the management review process to ensure the continuing suitability, adequacy, effectiveness and improvement of a management system
- Attempt to identify root causes of findings, if stated by the audit objectives;
- Consolidate similar findings made in different areas that were audited for the purpose of identifying trends.

If specified by the audit objectives, audit conclusions may lead to recommendations regarding improvements, business relationships, or future auditing activities.

6.4.8 Conducting the closing meeting

A closing meeting, facilitated by the audit team leader, should be held to present the audit findings and conclusions in such a manner that they are understood and acknowledged by the auditee. Participants in the closing meeting should include representatives of the auditee, and may also include the audit client and other parties. If applicable, the audit team leader should advise the auditee of situations encountered during the audit that may decrease the reliance that can be placed on the audit conclusions. If defined in the management system or by agreement with the person responsible for managing the audit programme, the participants should agree, on the time frame for an action plan to address audit findings.

For some audit situations, the meeting may be formal and minutes including records of attendance, should be kept. In other instances, for example, internal audits, the closing meeting is less formal and may consist solely of communicating the audit findings and audit conclusions.
As appropriate, the following should be explained in the closing meeting:

- advising the auditee that the audit evidence collected was based on a sample of the information available;
- the method of reporting, including any grading;
- the process of handling of audit findings and possible consequences;
- presentation of the audit findings in such a manner that they are understood and acknowledged by the auditee;
- any related post audit activities.

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

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

### 6.5 Preparing and distributing the audit report

#### 6.5.1 Preparing the audit report

The audit team leader should be responsible for the preparation and contents of the audit report.

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

- the audit objectives;
- the audit scope, particularly identification of the organizational and functional units or processes audited and the period of time covered;
- identification of the audit client;
- identification of audit team and auditee’s participants in the audit;
- the dates and locations where the audit activities were conducted;
- the audit criteria;
- the audit findings;
- the audit conclusions;
- a statement on the extent of the conformity to the audit criteria.

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

- the audit plan;
- a summary of the audit process, including the uncertainty and/or any obstacles encountered that may decrease the reliability of the audit conclusions;
- confirmation if the audit objectives have been accomplished within the audit scope in accordance with the audit plan;
- any areas within the audit scope not covered;
---

6.5.2 Distributing the audit report

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

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

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

6.6 Completing the audit

The audit is completed when all audit plan activities have been carried out or as otherwise agreed with the person responsible for managing the audit programme.

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

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

Lessons learned from the audit should be entered into the continual improvement process of the management system of the organization needing to conduct audits.

6.7 Conducting audit follow-up

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

The completion and effectiveness of the actions should be verified. This verification may be part of a subsequent audit.
7 Competence and evaluation of auditors

7.1 General

Confidence and reliance in the audit process depends on the competence of those individuals who are involved in planning and conducting the audits, including auditors and audit team leaders. Competence should be evaluated through a process that considers personal behaviours 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 7.3 are common to auditors of all management system disciplines; others are specific to auditors of specific management system disciplines.

The evaluation of auditors should be planned, implemented and documented in accordance with the audit programme to provide an outcome that is objective, consistent, fair and reliable. The evaluation process should include four main steps.

1) Determine the competence of audit personnel needed for the audit programme;
2) Establish the evaluation criteria;
3) Select the appropriate evaluation method;
4) Conduct the evaluation.

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

<table>
<thead>
<tr>
<th>Audit Team Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determination of training</td>
</tr>
<tr>
<td>Ongoing performance evaluation of auditors</td>
</tr>
</tbody>
</table>

Auditors should develop, maintain and improve their competence through continual professional development and regular participation in audits (see 7.5 and 7.6).

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

Audit team leaders should be evaluated against the criteria set out in 7.2.2.2 and 7.2.3.2.

7.2 Determine auditor competence to meet the needs of the audit programme

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

<table>
<thead>
<tr>
<th>Size, Nature, and Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management System Disciplines to be Audited</td>
</tr>
<tr>
<td>Objectives and Extent of the Audit Programme</td>
</tr>
<tr>
<td>Other Requirements</td>
</tr>
<tr>
<td>Role of the Audit Process</td>
</tr>
<tr>
<td>Complexity of the Management System</td>
</tr>
<tr>
<td>Uncertainty in Achieving Audit Objectives</td>
</tr>
</tbody>
</table>
This information should be matched against that listed in 7.3.1, 7.3.2 and 7.3.3.

### 7.2.1 Personal behaviours

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

- ethical, i.e. fair, truthful, sincere, honest and discreet;
- open minded, i.e. willingness to consider alternative ideas or points of view;
- diplomatic, i.e. tact in dealing with people;
- observant, i.e. active observation of physical surroundings and activities;
- perceptive, i.e. aware of and able to understand situations;
- adaptable, i.e. adjust readily to different situations;
- tenacious, i.e. persistence, focus on achieving objectives;
- decisive, i.e. reaching timely conclusions based on logical reasoning and analysis;
- self reliant, i.e. acting and functioning independently while interacting effectively with others;
- acting with fortitude i.e. willing to act responsibly and ethically even though these actions may not always be popular and may sometimes result in disagreement or confrontation;
- well organized, i.e. exhibiting effective time management, prioritization, planning and efficiency;
- open to improvement, i.e. learning from situations, striving for better audit results;
- culturally sensitive, i.e. observe and respect cultural traditions of the auditee;
- team player i.e. works well with other audit team members.

### 7.2.2 Knowledge and skills

#### 7.2.2.1 Generic knowledge and skills of management system auditors

Auditors should have knowledge and skills in the following areas:

a) Audit principles, procedures and techniques: to enable the auditor to apply those appropriate to different audits and ensure that audits are conducted in a consistent and systematic manner. An auditor should be able:

- to apply audit principles, procedures, methods and techniques;
- to plan and organize the work effectively;
- to conduct the audit within the agreed time schedule;
- to prioritize and focus on matters of significance;
- to collect information through effective interviewing, listening, observing and reviewing documents, records and data;
to understand the appropriateness and consequences of using sampling techniques for auditing;

to verify the accuracy of collected information;

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

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

to use work documents to record audit activities;

to prepare audit reports;

to maintain the confidentiality and security of information;

to communicate effectively, orally and in writing (including provisions for use of interpreters and translators);

to understand the types of risks associated with auditing.

b) Management system and reference documents: to enable the auditor to comprehend the scope of the audit and apply audit criteria. Knowledge and skills in this area should cover:

the application of management systems to different organizations;

interaction between the components of the management system;

specific management system standards, applicable procedures or other management system documents used as audit criteria;

recognizing the hierarchy of reference documents;

application of the reference documents to different audit situations;

control and protection of information, data, documents and records;

organizational context: to enable the auditor to comprehend the auditee's structure, business and management practices. Knowledge and skills in this area should cover;

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

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

cultural and social aspects of the auditee.

c) Applicable legal and other requirements that apply to the auditee to enable the auditor to work within, and be aware of, the organization's legal and contractual requirements. Knowledge and skills specific to the jurisdiction and/or auditee's activities and products should cover:

laws and regulations;

basic legal terminology;

contract and liability.
7.2.2.2 Generic knowledge and skills of audit team leader

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

- balance the strengths and weaknesses of the individual audit team members;
- develop a harmonious working relationship among the team members;
- manage the audit process, including:
  - planning the audit and making effective use of resources during the audit;
  - managing the uncertainty of achieving audit objectives;
  - protecting the safety and health of the audit team members during the audit, including ensuring compliance of the auditors with the relevant health, safety and security requirements;
  - organizing and directing the audit team members;
  - providing direction and guidance to auditors-in-training;
  - preventing and resolving conflicts, as necessary;
- represent the audit team in communications with the audit client and auditee;
- understand and respect the experts’ opinions;
- lead the audit team to reach the audit conclusions; and
- prepare and complete the audit report;

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

An auditor who intends to audit a specific type of management system should have the discipline and sector specific knowledge and skills that are appropriate for auditing the particular type of management system and industry sector.

Each auditor in the audit team does not need to have the same competence; however, the overall competence of the audit team needs to be sufficient to meet the audit objectives.

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

- understanding of the discipline and sector specific management system requirements and principles, and their application;
- understanding applicable legal and other requirements relevant to the discipline and sector: to enable the auditor to work within, and be aware of, the requirements those apply to the organization being audited. Knowledge and skills specific to the jurisdiction and/or auditee’s obligations, activities and products;
- understanding of the information (e.g. body of knowledge) that is fundamental to the business and technical processes, science and technology underlying the discipline sufficient to enable the auditor to evaluate management system elements associated with the discipline;
- understanding of discipline specific knowledge related to the particular sector, nature of operations, or workplace being audited sufficient for the auditor to evaluate the auditee’s activities, services, processes, products and services;
understanding risk management principles, methods and techniques relevant to the discipline and sector to enable the auditor to examine the auditee’s approach to managing risk.

NOTE Detailed guidance of specific knowledge and skills for selected disciplines are provided in Annexes A and B.

7.2.3 Education, work experience, training and audit experience of auditors

7.2.3.1 Auditors

Auditors should have completed an education sufficient to acquire the knowledge and skills described in 7.3. They should have work experience that contributes to the development of the knowledge and skills described in 7.3.3. This work experience should be in a technical, managerial or professional position involving the exercise of judgment, decision making, problem solving and communication with managers, professionals, peers, customers and/or other interested parties. Part of the work experience should be in a position where the activities undertaken contribute to the development of knowledge and skills in a management system for which they intend to audit.

They should have completed training in audit principles, procedures and techniques.

The should acquire audit experience under the supervision of an audit team leader.

7.2.3.2 Audit team leaders

An audit team leader should have acquired additional audit experience to develop the knowledge and skills described in 7.3.2. This additional experience should have been gained by working under the direction and guidance of an audit team leader.

7.2.3.2.1 Auditors who audit combined or integrated management systems

Auditors who intend to become an audit team member in the audit of combined or integrated management systems should have:

- the competence necessary to audit at least one management system discipline forming part of the combined or integrated management systems, as long as the audit team includes auditors with competence for all disciplines;
- an understanding of the interaction and synergy between the different management systems;

An audit team leader conducting audits of combined or integrated management systems should meet the above recommendations and have discipline specific competence to coordinate the auditing of multiple disciplines.

7.3 Establish the evaluation criteria

The criteria may be qualitative (such as having demonstrated personal behaviours, 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 Select the appropriate evaluation method

The evaluation should be conducted using two or more of the methods selected from those in Table 1. In using Table 1, the following should be noted:

- the methods outlined represent a range of options and may not apply in all situations;
- the various methods outlined may differ in their reliability;
— typically, a combination of methods should be used to ensure an outcome that is objective, consistent, fair and reliable.

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

Table 1 — Possible Evaluation Methods

7.5 Conduct the evaluation

In this step the information collected about the person is compared against the criteria set in 7.3. Where a person expected to participate in the audit programme does not meet the criteria, additional training, work and/or audit experience, and a subsequent re-evaluation should be performed.

Annex B provides hypothetical examples.

7.6 Maintenance and improvement of competence

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

The organization needing to conduct audits should establish suitable mechanisms for the continual evaluation of performance of the auditors, audit team leaders and those responsible for managing the audit programme.

The continual professional development activities should take into account results of post audit reviews, changes in the needs of the individual and the organization needing to conduct audits, the practice of auditing, standards and other requirements.
Figure 4 — Auditor competence evaluation
Annex A
(Informative)

Discipline-specific knowledge and skills of auditors

A.1 General

The following sub-clauses give generic examples of discipline-specific knowledge and skills for auditors of management systems, intended as guidance to assist those responsible for managing the audit programme(s) to select or evaluate auditors. Other examples of discipline-specific knowledge and skills for auditors may be developed for management systems other than these examples. It is suggested that such examples follow the same general structure where possible in order to ensure comparability.

A.2 Discipline-specific knowledge and skills of auditors – Quality

A.2.1 Understanding of the quality management system requirements – principles and their applications:

— Quality management system principles and their application.
— Management system requirements for the quality standard being audited against.

A.2.2 Appreciation of legal and other requirements relevant to quality sufficient to enable the auditor to evaluate the quality management system:

— Legal and other requirements dealing with quality and conformity assessment.
— Sector-specific Legal and other requirements dealing with quality, if applicable.
— Legal and other requirements dealing with product safety, labelling, prohibited substances, product life cycle, and acceptable work environment.
— Industry and trade association best practices documents.
— Guidance from regulatory bodies.
— Customer agreements.

A.2.3 Understanding of the application of quality techniques sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples include:

— Process control (e.g. statistical process control).
— Risk techniques for determining risk (e.g. Failure mode and effect analysis – see ISO/IEC 31010).
A.2.4 Understanding of the information (e.g. body of knowledge) that is fundamental to the processes, science and technology underlying quality sufficient to enable the auditor to evaluate management system elements associated with the discipline:

— Quality terminology.
— Measurement science and monitoring techniques.
— Statistics.
— General characteristics of processes and products, including services.

A.2.5 Understanding of quality knowledge related to the particular resources, assets sector, operation, or workplace being audited for the auditor to evaluate the auditee’s activities, functions, processes, products and services:

— Sector terminology.
— Fundamental concepts and principals of operations of the sector.
— Sector-specific processes and practices.
— Appreciation of interested parties’ expectations (e.g. expectations of the customers of the product/service).

A.3 Discipline-specific knowledge and skills of auditors – Environmental

A.3.1 Understanding of environmental management system requirements and principles, and their application:

— Environmental management system principles and their application.
— Requirements of the environmental management system standard being audited against.

A.3.2 Appreciation of legal and other requirements relevant to environment sufficient to enable the auditor to evaluate the environmental management system:

— Legal and other requirements dealing with the environment.
— Process-specific legal and other requirements dealing with environmental protection, pollution prevention and resource efficiency.
— Legal and other requirements dealing with labelling, use of hazardous substances, product life cycle, product stewardship.
— Industry and trade association best practices documents.
— Guidance from regulatory bodies.
— Customer and interested parties agreements (e.g. community, non-governmental organizations, local authorities).
A.3.3 Understanding of environmental techniques sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples include:

- Risk techniques for determining risk (e.g. environmental aspects/impact evaluation, including methods for evaluating significance).
- Life cycle assessment.
- Environmental performance evaluation.
- Pollution control and sustainability practices (e.g. best available technique assessment for pollution control or energy efficiency).

A.3.4 Understanding of information (e.g. body of knowledge) that is fundamental to the processes, science and technology underlying environment sufficient to enable the auditor to evaluate management system elements associated with the discipline:

- Environmental terminology.
- Source reduction, waste minimization and sustainability (e.g. Carbon footprint and greenhouse gas emissions).
- Measurement science and monitoring techniques.
- Statistics.
- Impact of human activities on the environment, including nuisance, cultural heritage, community impacts.
- Interaction of ecosystems and biodiversity.
- Environmental media (e.g. air, water, land).
- Management of natural resources (e.g. fossil fuels, water, flora and fauna).
- General measures of environmental protection.

A.3.5 Understanding of environmental knowledge related to the particular resources, sector, operation, or workplace being audited sufficient for the auditor to evaluate the auditee’s activities, functions, processes, products and services:

- Fundamental concepts and principals of operations of the sector.
- Sector-specific processes and practices.
- Interested parties’ expectations (e.g. expectations of the surrounding community).
- Environmental design.
- Key characteristics of processes and products, including services.
A.4 Discipline-specific knowledge and/or skills of auditors – Occupational health and safety (OH&S)

A.4.1 Understanding of the OH&S management system requirements and principles, and their application:
- OH&S terminology.
- OH&S management system principles and their application.
- The OH&S Management system requirements from the standard (or requirements document) being used for audit.

A.4.2 Appreciation of legal and other requirements relevant to OH&S sufficient to enable the auditor to evaluate the OH&S management system:
- OH&S specific legal and other requirements.
- International conventions and treaties on OH&S.
- Regulatory frameworks and guidance from regulatory bodies.
- Legal and other requirements governing or affecting the organization’s (industrial, business or governmental) sector.
- Industry, trade association and other "best practices" documents.
- Employers’ association, labour union and customer agreements.

A.4.3 Understanding of the application OH&S techniques sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.

Examples include:
- Hazard identification, risk assessment, determining controls, and risk communication (the determining of controls should be based on the hierarchy of controls and should take account of the key success features of the different methods).
- The evaluation of health and human factors (including physiological and psychological factors) and the principles for assessing them.
- The development, use and evaluation of proactive and reactive performance measures and metrics.
- The evaluation of the different types and levels of OH&S competence required across an organization and the assessment of that competence.
- The investigation and evaluation of work-related incidents (including accidents and work-related illnesses).
- The encouragement of employee participation and involvement.
- The encouragement of employee wellness or well-being and self-responsibility (in relation to smoking, drugs, alcohol, weight related issues, exercise, stress, aggressive behaviour etc.), both during working hours and in their private lives.
A.4.4 Understanding of the information that is fundamental to the process, science and technology underlying the discipline to enable the auditor to evaluate management system elements associated with the discipline:

- The hazards and other factors affecting human performance in the workplace (such as physical, chemical and biological factors, as well as gender, age, handicap or other physiological, psychological or health factors).
- The interaction of humans to machines, processes and the work environment (including workplace, ergonomic and safe design principles, information and communication technologies (ICT)).
- Human behaviour and person to person interactions.
- The principles and practices for emergency planning, prevention, response and recovery.
- Methodologies for exposure monitoring and assessment.
- Methodologies for incident (including accident and work-related illnesses) investigations.
- Methodologies for monitoring and reporting on OH&S performance.
- Medical information (including medical data).
- Health-related information (including work-related exposure and illness monitoring data) – but giving especial consideration to confidential aspects.
- Systems of occupational exposure limit values (OEL’s).

A.4.5 Understanding of discipline-specific knowledge related to the particular resources, assets, sector, operation, or workplace being audited for the auditor to evaluate the auditee’s activities, services, products and processes:

- Processes, equipment, raw materials, hazardous substances, process cycles, maintenance, logistics, work flow organization, working practices, shift-scheduling, organizational culture, leadership, behaviours, and other issues specific to the operation or sector.
- Typical hazards and risks, including health and human factors, for the sector.
- Sector-specific legal and other requirements.
- Sector-specific OH&S risk assessment, risk control and OH&S management techniques.
- Relevant indicators for proactive and reactive performance measures and metrics for the sector.

A.5 The discipline-specific knowledge and/or skills of auditors – Resilience, security, preparedness and continuity (RSPC) management

A.5.1 Understanding of RSPC management system requirements – principles and applications:

- Management system requirements for the RSPC standards being audited against

A.5.2 Appreciation of applicable legal and other requirements relevant to RSPC sufficient to enable the auditor to evaluate the RSPC management system:

- Discipline specific legal and other requirements.
Statutes, regulations and case law governing or affecting the industry sector and the protection of tangible and intangible assets (including people, property, the environment, information, intellectual property and reputation).

Industry and trade association best practices.

Guidance from regulatory bodies.

Supply chain obligations and expectations.

Labour union and customer agreements.

**A.5.3 Understanding of the application of RSPC techniques that enable the auditor to examine the management system and generate appropriate audit findings and conclusions.**

Examples include:

- Asset identification and valuation.
- Risk assessment (risk identification, analysis, evaluation).
- Risk treatment (adaptive, proactive and reactive measures).
- Developing performance measures and metrics.
- Information integrity and sensitivity.
- Exercise and testing methodologies.
- Legal and other requirements pertaining to the collection and preservation of evidence.

**A.5.4 Understanding of the information (body of knowledge) that is fundamental to the processes, science and technology underlying RSPC sufficient to enable the auditor to evaluate management system elements associated with the discipline:**

- Risk, resilience, security, preparedness, crisis, emergency, continuity and recovery management terminology.
- Intelligence.
- Principles of risk identification, analysis and evaluation, and risk communication.
- Asset protection and physical security.
- Prevention, deterrence, and security risk management.
- Incident mitigation, response and crisis management.
- Business/operational, continuity, emergency, recovery, management.
- Emergency communications and services.

**A.5.5 Understanding of RSPC knowledge related to the particular resources, assets, sector, operation, or workplace being audited for the auditor to evaluate the auditee’s activities, functions, processes, products and services:**

- RSPC related asset, sector and operations terminology.
ISO/DIS 19011

1311 — Asset identification, valuation and criticality analysis.
1312 — Asset management.
1313 — Information security and management.
1314 — Interested parties’ needs.
1315 — Supply chain roles and interactions.
1316 — Sector-specific processes and practices.
1317 — Risk treatment and control technologies, techniques and process.

A.6 The discipline-specific knowledge and/or skills of auditors - Discipline: Transportation safety management

A.6.1 Understanding of the transportation safety management system requirements – principles and applications:

— Management system requirements for the safety management standards and/or regulations being audited against.

A.6.2 Appreciation of legal and other requirements to which the auditee subscribes relevant to transportation safety management sufficient to enable the auditor to evaluate the transportation safety management system:

— Legal and other requirements dealing with safety management requirements (aviation, railway, marine, road traffic).

— Statutes, regulations and case law governing or affecting the transportation sector and the protection of tangible and intangible assets (including people, property, the environment, information, intellectual property and reputation).

— Sector specific industry association best practices.

— Sector specific guidance from regulatory bodies.

— Sector specific supply chain requirements.

— Labour union and customer agreements.

A.6.3 Understanding of application of transportation safety management techniques that enable the auditor to examine the management system and generate appropriate audit findings and conclusions

Examples include:

— Risk assessment and mitigation.

— Human Factor techniques.

— Developing proactive and reactive performance measures and metrics.

— Understanding safety culture approach.
A.6.4 Understanding of the information (body of knowledge) that is fundamental to the processes, science and technology underlying transportation safety management to enable the auditor to evaluate management system elements associated with the discipline:

- Safety management terminology.
- Potential hazards and other workplace factors affecting safety.
- Interaction of humans, machines, processes and the work environment.
- Methodologies for incident investigations.
- Methodologies for monitoring safety performance.
- Human behaviour and interaction.

A.6.5 Understanding of transportation safety management knowledge related to the particular resources, assets, sector, operation or workplace being audited for the auditor to evaluate the auditee’s activities, functions, processes, products and services:

- Safety management related asset and operations terminology (aviation, railway, marine, road traffic).
- Industry specific technology knowledge (aviation, railway, marine, road traffic).
- Industry specific processes and operating procedures (aviation, railway, marine, road traffic).
- Industry specific global safety network setup.

A.7 Discipline-specific knowledge and skills of auditors – Records

A.7.1 Understanding of management system for records – principles, requirements and their application

- Management system for records principles and their application.
- Requirements of the management system for records standard being audited against.

A.7.2 Appreciation of business, legal and other requirements relevant to records sufficient to enable the auditor to evaluate the management system for records:

- Legal and other requirements dealing with general business requirements with records implications, e.g. corporation law, finance and taxation law.
- Legal and other requirements relating specifically to evidence, records and archives; access, privacy, data and information protection, electronic commerce and communication.
- Guidance from regulatory bodies.
- Industry sector–specific legal and other requirements dealing with records requirements.
- Industry and trade association best practices documents and international records management standards and guidelines.
Identifiable expectations of the community about what is acceptable behaviour for the specific sector or organization, including good governance, the proper control of fraudulent or malicious behaviour, and transparency in decision making.

Identifiable requirements of business areas interested in evidence-based process and working in a consistent and recognized manner, e.g. risk management, security management, quality management, business continuity management, auditing management, environmental management, social responsibility, etc.

A.7.3 Understanding of techniques applicable to the management system for records sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions

Examples include:

- Developing performance measures and metrics.
- The investigation and evaluation of records practices through interviewing, observation and validation.
- Sample analysis of records created in business processes.
- Risk assessment (e.g., assessment of risks through failure to create, maintain and control adequate records of the organization's business processes).
- The performance and adequacy of records processes to create, capture and control records.
- Assessment of the adequacy and performance of records system/s (including business systems to create and control records), the suitability of technological tools used, and facilities and equipment established.
- Evaluation of the different levels records competence required across an organization and the assessment of those competence.

A.7.4 Understanding of information (e.g. body of knowledge) that is fundamental to the processes, science and technology underlying records management sufficient to enable the auditor to evaluate management system elements associated with the discipline:

- Records, records management processes, and management systems for records terminology.
- Significance of the content, context, structure, representation and control information (metadata) required to define and manage records and records systems.
- Methodologies for developing records-specific instruments.
- Understanding of technologies used for creation, capture, conversion and migration, and long term preservation of electronic/digital records.
- Key characteristics of records, records systems, records processes and controls.
- Identification and significance of the authorisation documentation for records processes.

A.7.5 Knowledge and understanding of records requirements and processes related to the particular resources, assets, sector, operation, or workplace being audited sufficient for the auditor to evaluate the auditee’s activities, functions, processes, products and services in relation to the management system for records:

- Fundamental concepts and principles of operations of the sector.
1410 — Sector-specific processes and practices and their implications for the key characteristics of records, records system, records processes and controls of the sector.

1412 — Sector-specific risk assessment and legal and regulatory requirements.

1413 — Design of sector processes where records processes have been integrated with sector-specific processes.
Annex B
(Informative)

Examples of discipline specific evaluations of audit team competence

B.1 General.

The following sub-clauses give generic examples of discipline-specific competence for audit teams for management system auditing, intended as guidance to assist those responsible for managing the audit programme(s) to select or evaluate auditors.

The aim is to illustrate an approach for using the evaluation methodology described in Clause 7 of this International Standard.

The examples below provide discipline-specific competence evaluation criteria for audit teams consistent with existing management systems. Other examples of discipline-specific competence for audit teams may be developed for management systems other than these examples. It is suggested that such examples comprise the same general composition where possible in order to ensure comparability.

These examples are guidance for evaluating audit team competence and should not be considered requirements. This guidance provides examples that can be used in a fit-for-purpose audit team competence evaluation scheme.
### B.2 Application of the evaluation process for an audit team undertaking an internal audit of an aviation organization’s quality and environmental management systems

<table>
<thead>
<tr>
<th>Areas of competence</th>
<th>Personal behaviours and skills</th>
<th>Evaluation criteria</th>
<th>Evaluation method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personnel behaviours</strong></td>
<td>Ethical, open-minded, diplomatic, observant, perceptive, adaptable, tenacious, decisive, self-reliant, acting with fortitude, well organized, open to improvement, culturally sensitive, team player.</td>
<td>Satisfactory performance in the workplace</td>
<td>Performance evaluation.</td>
</tr>
<tr>
<td><strong>Generic knowledge and skills</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Audit principle, procedures, processes and techniques</strong></td>
<td>Conduct an audit according to in-house procedures, communicating with known workplace colleagues.</td>
<td>Successfully completed an in-house auditor training course.</td>
<td>Review of training record.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performed satisfactorily in X audits as a member of an internal audit team.</td>
<td>Observation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review of training records.</td>
<td>Peer review.</td>
</tr>
<tr>
<td><strong>Management systems and other reference documents</strong></td>
<td>Apply the relevant parts of the quality and environmental management system manual and related procedures.</td>
<td>Read and understood procedures relevant to the audit objectives, scope and criteria.</td>
<td>Review of training records.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review of training records.</td>
<td>Interview.</td>
</tr>
<tr>
<td><strong>Organizational situations</strong></td>
<td>Describe the auditee’s local structure and culture and any demarcation issues.</td>
<td>Worked for the auditee for at least five years at supervisor or managerial level.</td>
<td>Review of employment records.</td>
</tr>
<tr>
<td><strong>Legal and other requirements</strong></td>
<td>Identify and understand the application of the relevant laws and regulations related to product quality and the environment.</td>
<td>Successfully completed a training course on the laws relevant to the activities, process and/or products and services the subject of this</td>
<td>Review of training records.</td>
</tr>
</tbody>
</table>
### Risk assessment

- Identify and understand the application of the risk assessment process to the auditee’s activities.
- Completed a training course on risk assessment or conducted risk assessments as part of a work related activity.
- Review of training records.
- Interview.
- Review of employment records.

### Industry (sector) specific skills

#### Terminology
- Knowledge and understanding of aircraft engineering terminology.
- Knowledge of Emissions from machining processes, waste oil, plating effluent.
- Worked for an aviation company for minimum of five years.
- Employed as the wastewater treatment supervisor for at least three years.
- Review of training record.

#### Process
- Knowledge of engineering processes such as machining, welding, heat treatment.
- Knowledge of waste water, air emissions from machining.
- Worked as an engineer within the aviation sector for not less than five years.
- Completed an indoor air quality training course.
- Verification of professional qualification Supervisor Observation.

#### Technology
- Knowledge of NCM, NDI and X ray.
- Knowledge of air abatement techniques, heavy metal waste water treatment.
- Worked as in a technical capacity as a production supervisor or similar for at least two years.
- Acted as assistant facilities manager for not less than two years.
- Employment record.
- Observation.
<table>
<thead>
<tr>
<th>Organization specific skills</th>
<th>Knowledge and understanding of landing gear, hydraulic servo’s, pumps, cavitations. Understand gaseous emissions from machining processes. Knowledge of miscible oils, surfactants.</th>
<th>Worked for at least five years in supervisory role in the aviation sector. Professional recognition or certification gained through study or registration by an accredited body. Undertaken 3 prior audits of a manufacturing facility. Attended a hazardous chemicals training course.</th>
<th>Employment record. Review of training record.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminology</td>
<td>Knowledge of continuous machining, use of CMM, laser alignment techniques. Knowledge and understanding of methods of treatment of effluents and discharges.</td>
<td>Worked for at least five years in supervisory role in the aviation sector. Professional recognition or certification gained through study or registration by an accredited body. Acted as assistant facilities manager for not less than two years.</td>
<td>Employment record. Review of training record.</td>
</tr>
<tr>
<td>Process</td>
<td>Knowledge of the application laser technology, CMM. Knowledge and understanding of platting discharges and their impact on local water courses.</td>
<td>Worked for at least five years in supervisory role in the aviation sector. Professional recognition or certification gained through study or registration by an accredited body.</td>
<td>Employment record. Review of training record.</td>
</tr>
</tbody>
</table>
### Statistical techniques

| Analytical ability to apply Cp Six Sigma techniques. |
| Knowledge and understanding of statistical techniques applied to waste water treatment, numerical comparison of discharge levels to legal requirements. |
| Six Sigma black belt |
| Professional recognition or certification gained through study or registration by an accredited body. |
| Completed wastewater discharge training course. |
| Completed a statistical training course. |

**Employment record.**

**Review of training record.**

### Products/services

| Knowledge of servo’s, axles, shock absorbers. |
| Knowledge end of life protocols. |
| Completed three months working in the Sales and Marketing department. |
| Professional recognition or certification gained through study or registration by an accredited body. |

**Employment record.**

### Risk

| Knowledge and understanding of process errors, forging impurities. |
| Knowledge of environmental risks associated |
| Undertaken a risk management-training course. Assisted in the preparation FMEA studies. |
| Professional recognition or certification gained through study or registration by an accredited body. |

**Employment record.**
| Interested parties | Aircraft manufacturers.  
Knowledge of the local regulators re standards and enforcement. | Formerly on staff of the customer complaints department.  
Previous liaison with regulator. | Employment record.  
Review of training record. |
|-------------------|-----------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------|
| Management system specific skills (quality & environment) | Quality control, assurance, $C_p$, concentricity measurement.  
Aspects and impacts, control methods, resource efficiency. | Six sigma black belt.  
Completed an ISO 17024 accredited quality or environmental management system auditor training course.  
Undertaken aspect/impact training course. Applied training course within the company. | Employment record.  
Review of training record. |
| Terminology | Application of auditee’s processes applied in different management stages.  
Knowledge of multiple discharges and their synergy. | Worked for at least five years in supervisory role in the aviation sector.  
Attended a hazardous chemicals training course.  
Completed waste water discharge training course.  
Completed an indoor air quality training course. | Employment record.  
Review of training record. |
<table>
<thead>
<tr>
<th>Technology</th>
<th>Knowledge of technologies used across the auditee. Knowledge of technologies used across the auditee and its environmental interaction.</th>
<th>Worked for at least five years in supervisory role in the aviation sector. Undertaken 3 prior audits of a manufacturing facility.</th>
<th>Employment record. Review of training record.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistical techniques</td>
<td>Analytical ability to interpret statistical results.</td>
<td>Six sigma black belt.</td>
<td>Employment record.</td>
</tr>
</tbody>
</table>
## B.3 Application of the evaluation process for an audit team undertaking an internal audit of an event management organization’s Quality and OH&S management systems

<table>
<thead>
<tr>
<th>Areas of competence</th>
<th>Personal behaviours and skills</th>
<th>Evaluation criteria</th>
<th>Evaluation method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal behaviours</td>
<td>Ethical, open-minded, diplomatic, observant, perceptive, adaptable, tenacious, decisive, self reliant, acting with fortitude, well organized, open to improvement, culturally sensitive, team player.</td>
<td>Satisfactory performance in the workplace.</td>
<td>Performance evaluation.</td>
</tr>
<tr>
<td>Generic knowledge and skills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit principles, procedures, processes and techniques</td>
<td>Ability to conduct an audit according to in-house procedures, communicating with known workplace colleagues and subcontractors.</td>
<td>Successfully completed an in-house or external auditor training course. Performed satisfactorily in 3 audits as a member of an internal audit team.</td>
<td>Review of training record. Observation. Peer review.</td>
</tr>
<tr>
<td>Management systems and other reference documents</td>
<td>Ability to apply the relevant parts of the Quality and OH&amp;S Management System Manual and related procedures.</td>
<td>Read and understood procedures relevant to the audit objective, scope and criteria.</td>
<td>Review of training records. Testing. Interview.</td>
</tr>
<tr>
<td>Organizational situations</td>
<td>Ability to describe the auditee’s local structure and culture and any demarcation issues.</td>
<td>Worked for the auditee for at least one year at supervisor or managerial level or a similar organization or been employed by the auditee as a consultant for one year.</td>
<td>Review of employment records.</td>
</tr>
<tr>
<td>Legal and other requirements</td>
<td>Identify and understand the application of the relevant laws and regulations related to product quality and OH&amp;S.</td>
<td>Successfully completed a training course on the laws relevant to the activities, process and/or products and services which are the subject of this audit or be registered as an OH&amp;S inspector.</td>
<td>Review of training records.</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Understanding the principles of hazard identification, risk assessment and</td>
<td>Completed a training course on risk assessment or conducted risk</td>
<td>Review of training records.</td>
</tr>
<tr>
<td>Industry (sector) specific skills</td>
<td>Terminology</td>
<td>Knowledge of generic terminology for the sector such as events, banquets, exhibitor, venue, exhibition, main contractor.</td>
<td>Employed in the sector or that similar nature for at least one year as a project/site manager, or designer, or as a subcontractor supervisor.</td>
</tr>
<tr>
<td></td>
<td>Process</td>
<td>Generic knowledge on the items such as exhibition design, assembly process, non standard and custom design booths.</td>
<td>Employed in the sector or that similar nature for at least one year as a project/site manager, or designer, or as a subcontractor supervisor.</td>
</tr>
<tr>
<td></td>
<td>Technology</td>
<td>Understanding knowledge of computer aided design (CAD) tools, audio visual, electrical and electronic equipment and its compatibility.</td>
<td>Electrical license or certificate in low voltage equipment or equivalent. Completed a training course on CAD or worked as designer for a similar organization for at least one year.</td>
</tr>
</tbody>
</table>

<p>| Organization specific skills | Terminology | Generic knowledge on the items such as banquet, product launch, exhibition, organizer, exhibitor. | Employed in the sector or that similar nature for at least one year as a project/site manager, or designer, or as a subcontractor supervisor. | Employment record. |
| | Process | Spray painting, carpentry, graphic design, interior design and fit out. | Employed as a supervisor or site manager for painting, carpentry, electrical installation or person with 3 years work experience in the relevant discipline or that of similar nature. | Employment record. Observation. |
| | Technology | Hand and power tools. (Electrical or pneumatic), fastener usage, screws nails, nails gun, water based spray painting, and glazing. | Employed as a supervisor or site manager for carpentry, painting, electrical installation or person with 3 years work experience in the relevant discipline or that of similar nature. | Employment record. Observation. |
| | Statistical techniques | Not applicable. | | |</p>
<table>
<thead>
<tr>
<th>Products/services</th>
<th>Knowledge of auditee’s services such as booth design, interior fit out, event set ups.</th>
<th>Employed in sales department at this or similar organization, worked as a contractor setting up events.</th>
<th>Employment record.</th>
</tr>
</thead>
</table>
| Risk              | Understanding OH&S risks associated with the location at which the services are offered. | Conducted or reviewed risk assessments in this sector or a similar sector for not less than one year. | Employment record.  
Interview. |
| Interested parties | Exhibitors, venue, organizer, subcontractors, local regulators. | Worked in the sector for not less than 12 months in a managerial or supervisory role.  
Previous liaison with regulator. | Employment record. |
| Management system specific skills (quality & occupational health and safety) | Quality control, assurance, customer satisfaction.  
OH&S hazards and risks, control measures. | Undertaken courses or training in quality control or quality assurance tool, or OH&S hazard identification, and applied training within the organization. | Employment record.  
Review of training record. |
| Terminology       | Application of auditee’s activities and processes utilized in different stages of the event management. | Worked for at least two years in supervisory role in the sector. | Employment record. |
| Process           | Generic knowledge such as CAD techniques applied to booth design or of a similar nature. | Worked as designer for at least two years in the sector or of similar nature. | Employment record. |
| Technology        | Statistical techniques | | |
| Risk              | Understand the auditee’s risk assessment processes.  
Understanding of physical, chemical, biological and psychological hazards and | Undertaken a risk management-training course.  
Undertaken courses or training in hazard and risk control and applied training | Employment record.  
Review of training record. |
**B.4 Application of the evaluation process for an auditor in a hypothetical resilience, security, preparedness and/or continuity management internal audit programme**

<table>
<thead>
<tr>
<th>Areas of competence</th>
<th>Personal behaviours, and knowledge and skills</th>
<th>Evaluation criteria</th>
<th>Evaluation methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal behaviours</td>
<td>Ethical, open-minded, diplomatic, observant, perceptive, adaptable, tenacious, decisive, self reliant, acting with fortitude, well organized, open to improvement, culturally sensitive, team player.</td>
<td>Satisfactory performance in the workplace.</td>
<td>Performance evaluation.</td>
</tr>
<tr>
<td>Generic knowledge and skills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit principles, procedures and techniques</td>
<td>Ability to conduct an audit according to in-house procedures, communicating with known workplace colleagues.</td>
<td>Completed an ISO 17024 accredited personnel certification training programme.</td>
<td>Review of training records.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performed four audits as a member of an internal audit team.</td>
<td>Observation. Peer review.</td>
</tr>
<tr>
<td>Management system and reference documents</td>
<td>Ability to apply the relevant parts of the Management System Manual and related procedures.</td>
<td>Read and understood the procedures in the Management System Manual relevant to the audit objectives, scope and criteria.</td>
<td>Review of training records Testing. Interview.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Completed an ISO 17024 accredited resilience, security, preparedness or continuity management system personnel certification training programme.</td>
<td></td>
</tr>
<tr>
<td>Organizational situations</td>
<td>Ability to operate effectively within the auditee’s culture and organizational and reporting structure.</td>
<td>Worked for the auditee (or similar) for at least one year in a supervisory role.</td>
<td>Review of employment records.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Applicable legal and other requirements</td>
<td>Demonstrate knowledge of statutes, regulations and case law governing or affecting the industry sector and the protection of people, property and information including:</td>
<td>Completed training in the legal aspects of resilience, security, crisis, continuity and/or emergency management methods. Professional recognition or certification gained through study or registration by an accredited body. Implemented resilience, security, preparedness, response and recovery procedures as part of a work related activity in a decision making capacity for a minimum of 3 years. Security or continuity manager for a minimum of 5 years.</td>
<td>Review of training records, course content and results. Review of training and employment records.</td>
</tr>
<tr>
<td></td>
<td>— statutes, regulations and laws pertaining to personnel protection programmes, methods and techniques,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>— laws pertaining to protection requirements for proprietary information and intellectual property,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>— laws pertaining to the collection and preservation of evidence, and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>— laws pertaining to managing the background investigation process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Identify and understand the application of the risk assessment process to the auditee’s activities.</td>
<td>Completed a training course on risk assessment or conducted risk assessments as part of a work related activity for a minimum of 5 years.</td>
<td>Review of training records. Interview. Review of employment records.</td>
</tr>
<tr>
<td>Sector specific skills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminology</td>
<td>Knowledge of generic terminology such as security, intelligence, physical protection, surveillance, incidents, emergency response, continuity.</td>
<td>Former member of the defence or police forces. Employment in the security sector as a supervisor or manager for at least 5 years.</td>
<td>Employment record.</td>
</tr>
<tr>
<td>Process</td>
<td>Understanding of resilience processes such as protection, vetting/screening, surveillance and monitoring (physical and electronic), warnings, evacuations and continuity planning.</td>
<td>Former member of the defence or police forces. Employment in the security sector as a supervisor or manager for at least 5 years.</td>
<td>Employment record.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Technology</td>
<td>Surveillance technology, electronic identification, vehicle tracking, listening equipment, alarm systems, warming systems, intrusion detection, fire detection and control.</td>
<td>Former member of the defence, emergency services or police forces. Employment in the resilience-related sector as a supervisor or manager for at least 5 years.</td>
<td>Employment record.</td>
</tr>
<tr>
<td>Products/services</td>
<td>Ability to identify and value the tangible and intangible assets, the auditee's system (people, property, information, reputation, etc.). Ability to identify and evaluate supply chain role and commitments.</td>
<td>Completed training in the application of risk assessment and management methods. Professional recognition or certification gained through study or registration by an accredited body. Conducted risk assessments as part of a work related activity. Demonstrated work place experience. Training in supply chain management.</td>
<td>Review of training records, course content and results. Review of training and employment records. Observation.</td>
</tr>
<tr>
<td>Terminology</td>
<td>Knowledge of terminology related to risk management systems and treatments. Knowledge of terminology related to security management systems and treatments. Knowledge of terminology related to continuity management systems and treatments.</td>
<td>Completed training in the application of security risk, crisis, continuity and/or emergency management methods. Professional recognition or certification gained through study or registration by an accredited body. Conducted risk assessments as part of</td>
<td>Review of training records, course content and results. Review of training and employment records. Observation.</td>
</tr>
<tr>
<td>Processes</td>
<td>Technology</td>
<td>Statistical Techniques</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>Ability to identify the activities, functions, processes and products of an organization and evaluate the consequences of their disruption.</td>
<td>Ability to comprehend the technological context in which the audit is being conducted including sector-specific terminology, technical characteristics of processes and products, including services, and sector-specific processes and practices. Ability and understand technical risk treatment and control technologies (e.g. perimeter security protection technologies, alarms, access control, emergency management equipment)</td>
<td>Knowledge of quantitative and qualitative risk assessment methodologies (e.g. ISO 31010).</td>
<td></td>
</tr>
<tr>
<td>Completed training in the application of risk assessment and management methods. Professional recognition or certification gained through study or registration by an accredited body. Conducted risk assessments as part of a work related activity</td>
<td>Worked for at least five years in a supervisory role in the specific industry sector. Professional recognition or certification gained through study or registration by an accredited body. Undertaken four prior audits of an appropriate manufacturing, transport, or distribution facility. Attended an industry-training course.</td>
<td>Completed training in the application of risk assessment and management methods. Professional recognition or certification gained through study or registration by an accredited body.</td>
<td></td>
</tr>
</tbody>
</table>
| Risk | Knowledge of risk assessment and impact analysis to examine efficiency risk management systems and treatments. | Completed training in the application of risk assessment and management methods.  
Professional recognition or certification gained through study or registration by an accredited body.  
Conducted risk assessments as part of a work related activity.  
Demonstrated work place experience. | Review of training records, course content and results.  
Review of training and employment records.  
Observation. |
| Interested parties | Ability to identify appropriate interested parties including: customers, clients, partners, employees, shareholders, owners, vendors, the local community, first responders, government agencies, and regulators. | Completed training in the application of risk assessment and management methods.  
Professional recognition or certification gained through study or registration by an accredited body.  
Conducted risk assessments as part of a work related activity. | Review of training records, course content and results.  
Review of training and employment records.  
Observation. |
| Management system specific skills |
| Terminology | Knowledge of terminology of the disciplines of risk, resilience, security, preparedness, crisis, response, emergency, continuity, emergency and disaster management including related technologies. | Completed training in the application of security risk, crisis, continuity and/or emergency management methods.  
Professional recognition or certification gained through study or registration by an accredited body. | Review of training records, course content and results.  
Review of training and employment records. |
| Intelligence | Knowledge of information and intelligence sources, warning systems and their interpretation. | Completed training in the application of risk assessment and management methods.  
Professional recognition or certification gained through study or registration by an accredited body.  
Experience as security or continuity manager for 5 years. | Review of training records, course content and results.  
Review of training and employment records. |
| --- | --- | --- | --- |
| Management of Risk | Ability to understand:  
— risk, resilience, security, preparedness and continuity management principles and their application;  
— concepts to develop, manage or conduct risk assessments and impact analyses to determine the probable frequency, severity, and consequences of natural and man-made disasters and criminal activity on the auditee’s profitability, resilience and/or ability to deliver products/services;  
— methodologies to control and manage risk and improve security, preparedness, continuity, recovery and loss prevention systems on a continuous basis through the use of surveys, review and assessment;  
— development and management of external relations programmes with | Completed training in the application of risk assessment and management methods.  
Professional recognition or certification gained through study or registration by an accredited body.  
Conducted risk assessments as part of a work related activity. | Review of training records, course content and results.  
Review of training and employment records. |
<table>
<thead>
<tr>
<th><strong>ISO/DIS 19011</strong></th>
</tr>
</thead>
</table>
| public sector law enforcement or other external organizations to assist in the achievement of loss prevention objectives; and

— development and implementation of employee security, preparedness and continuity awareness programmes to achieve organizational goals and objectives. |
| Completed training in the application of physical security management methods. |
| Professional recognition or certification gained through study or registration by an accredited body. |
| Implemented physical security analysis and procedures as part of a work related activity in a decision-making capacity for a minimum of 5 years. |
| Review of training records, course content and results. |
| Review of training and employment records. |

| **Physical Security** | Ability to understand the fundamental relationships needed to manage and/or evaluate the current status of the physical security, fire detection and emergency and/or restoration capabilities. |
|---------------------------------------------------------------|
| Completed training in the application of physical security management methods. |
| Professional recognition or certification gained through study or registration by an accredited body. |
| Implemented physical security analysis and procedures as part of a work related activity in a decision-making capacity for a minimum of 5 years. |
| Review of training records, course content and results. |
| Review of training and employment records. |

| **Emergency Practices** | Ability to understand the mitigation of potential consequences of disruptive incidents and emergency situations by identifying and prioritizing potential hazards and risks and developing plans to manage exposure to loss. |
|------------------------------------------------------------------|
| Completed training in the application of security risk, crisis, continuity and/or emergency management methods. |
| Professional recognition or certification gained through study or registration by an accredited body. |
| Implemented preparedness, response and recovery procedures as part of a work related activity in a decision-making capacity for a minimum of 5 years. |
| Experience as a member of the |
| Review of training records, course content and results. |
| Review of training and employment records. |
| Personnel Security | Ability to understand the development, implementation, management, and evaluation of policies, procedures, programmes and methods for protection of human assets and to provide a secure work environment. | Completed training in the application of security risk, crisis, continuity and/or emergency management methods.  
Professional recognition or certification gained through study or registration by an accredited body.  
Implemented security, preparedness, response and recovery procedures as part of a work related activity in a decision-making capacity for a minimum of 5 years.  
Security manager for a minimum of 5 years.  
Experience as a member of the emergency response team for a minimum of 3 years. | Review of training records, course content and results.  
Review of training and employment records. |
|-------------------|-------------------------------------------------|---------------------------------------------------------------------------------|------------------------------------------------|
| Information Security | Ability to understand the development and implementation of policies, procedures and standards to ensure information is evaluated and protected against all forms of unauthorized/inadvertent access, use, disclosure, modification, destruction or denial. | Completed training in the application of information security management methods.  
Professional recognition or certification gained through study or registration by an accredited body.  
Implemented information and recovery procedures as part of a work related activity in a decision-making capacity for a minimum of 3 years.  
Information security manager for a minimum of 3 years. | Review of training records, course content and results.  
Review of training and employment records. |
minimum of 5 years.
C.1 Applying audit methods

An audit can be performed using a range of audit methods. An explanation of common 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 (sites). Available auditor competence and any uncertainty arising from the application of audit methods should also be considered. Applying a variety and combination of different audit methods can optimize the efficiency and effectiveness of the audit process and its outcome.

Performance of an audit involves an interaction among individuals with the management system(s) being audited and the technology used to conduct the audit. Table 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.

<table>
<thead>
<tr>
<th>Extent of involvement between the auditor and the auditee</th>
<th>Location of the auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On-Site</td>
</tr>
<tr>
<td>Human Interaction.</td>
<td></td>
</tr>
<tr>
<td>— Conducting interviews.</td>
<td></td>
</tr>
<tr>
<td>— Filling checklists and questionnaires with auditee participation.</td>
<td></td>
</tr>
<tr>
<td>— Document review with auditee participation.</td>
<td></td>
</tr>
<tr>
<td>No Human Interaction</td>
<td></td>
</tr>
<tr>
<td>— Observation of work performed.</td>
<td></td>
</tr>
<tr>
<td>— Site visit.</td>
<td></td>
</tr>
<tr>
<td>— Filling checklists.</td>
<td></td>
</tr>
<tr>
<td>— Sampling (e.g. products).</td>
<td></td>
</tr>
<tr>
<td>— Document review (e.g. records).</td>
<td></td>
</tr>
<tr>
<td>— Via communication means:</td>
<td></td>
</tr>
<tr>
<td>— Conducting interviews.</td>
<td></td>
</tr>
<tr>
<td>— Filling checklists and questionnaires.</td>
<td></td>
</tr>
<tr>
<td>— Document review with auditee participation.</td>
<td></td>
</tr>
<tr>
<td>— Document review.</td>
<td></td>
</tr>
<tr>
<td>— Observation of work performed via surveillance means.</td>
<td></td>
</tr>
</tbody>
</table>

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, independent of the distance.

Interactive audit activities involve interaction between the auditee’s personnel and the audit team. Non-interactive audit activities involve no human interaction with persons being audited but do involve interaction with equipment, facilities and documentation.

Table 1 – Applicable audit methods
NOTE Additional information on site visits is given in C.6 of this Annex;

The responsibility of the effective application of audit methods for any given audit remains with the person planning the audit. This will be either the person responsible for managing the audit programme or the audit team leader.

The feasibility of remote audits can depend on the level of confidence between auditor and auditee.

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

C.2 Sources of information

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

- interviews with employees and other persons;
- observations of activities and the surrounding work environment and conditions;
- documents, such as policies, objectives, plans, procedures, standards, instructions, licences and permits, specifications, drawings, contracts and orders;
- records, such as inspection records, minutes of meetings, audit reports, records of monitoring programmes and the results of measurements;
- data summaries, analyses and performance indicators;
- information on the auditee’s sampling programmes and on the procedures for the control of sampling and measurement processes;
- reports from other sources, for example, customer feedback, external surveys and measurements, other relevant information from external parties and supplier ratings;
- databases and web sites;
- simulations and modelling.

C.3 Conducting document review

The auditors should consider if:

a) the information in the documents provided is:

- complete (all expected content is contained in the document);
- correct (the content is compliant to other reliable sources such as standards and regulations);
- consistent (the document is consistent in itself and to related documents);
- current (the content is up to date).

b) the documents being reviewed cover the audit scope and are capable of providing sufficient information to support the audit objectives;

c) the use of information and communication technologies, depending on the audit methods should promote efficient conduct of the audit. Specific care is needed for information security due to applicable regulations on...
C.4 Preparing Work Documents

When preparing work documents, the audit-team should consider the following questions for each document:

- Which audit record will be created by using this work document?
- Which audit activity is affected by this particular work document?
- Who will be the user of this work document?
- What information is needed to prepare this work document?

For combined audits it is essential that thorough preparation of work documents avoids duplication of audit activities by:

- clustering of similar requirements from different criteria;
- synchronization of related checklists and questionnaires.

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

C.5 Sampling strategy considerations for audits

C.5.1 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 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 any audit sampling activity should be to provide a data set in which the auditor(s) can have sufficient confidence that the data will support the achievement of the audit objectives.

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

Audit sampling typically involves the following steps:

a) Determine the objectives of the sampling approach.
b) Identify the extent and composition of the population to be sampled.
c) Select a sampling method.
d) Determine the sample size to be taken.
e) Conduct the sampling activity.
f) Compile and evaluate the results.
In identifying the need for sampling, primary consideration should be given to the quality of the available data, as sampling poor data will not provide an accurate or useful result. The selection of an appropriate sample should be based on both the type of sample needed and the analysis required, e.g. to infer a particular behaviour pattern or draw inferences across a population.

If required, reporting on the sample selected should also take into account the sample size, selection methodology, estimates made based on the sample and the confidence level selected.

Sampling in an audit can be based on statistics or judgement.

C.5.2 Judgemental sampling

Judgemental sampling relies on the knowledge, skills and experience of the audit team, (see clause 7).

For judgement based sampling the following can be considered:

- previous audit experience within the audit scope;
- complexity of requirements (including legal requirements) to satisfy the objectives of the audit;
- complexity and interaction of the organizations processes and management system elements;
degree of change in technology, human factors and/or system;
— previous identified key risk areas and areas of improvement;
— output from monitoring of management systems;

A potential drawback to judgemental sampling is that there can be no scientific estimate of uncertainty or risk in the conclusions of the audit.

C.5.3 Statistical sampling

If there is a need to use statistical sampling methods the following apply:
— statistical sampling designs generally use a sample selection process combined with probability theory. The result is generally expressed in terms of attributed or variable based outcomes. Attribute sampling is where there are only two possible outcomes (e.g. correct or incorrect/pass or fail). Variable based is where the outcome may occur in a continuous range;
— sampling plans should be based on whether the auditor is expected to make an attribute based determination (pass/fail) regarding the proper implementation of the auditee’s controls, such as plans, procedures, work instruction etc., or is examining issues related to product quality and/or a number of food safety, safety and health or environmental incidents or security breaches where a variable based outcome is likely. All sampling plans should identify the level of risk (or its inverse - confidence level) that maybe present. For example a sampling risk of 5% (confidence level of 95%) means that there is a 1:20 chance that the auditor will not detect something that will materially affect the outcome of the audit.

C.6 Guidance for site visits and observations

To minimize interference with the auditee’s work processes and to ensure the safety of the audit team during a site visit or observation, the following should be considered:

C.6.1 Planning the visit
— ensure permission and access to those parts of the site or the work location, to be visited in accordance with the audit scope;
— provide adequate information (e.g. briefing) to auditors on security, health (e.g. quarantine), occupational health and safety matters and cultural norms for the site visit including requested and recommended vaccination and clearances, if applicable;
— ensure use of personal protective equipment (PPE) for auditors and arrange with auditee who will provide it, if applicable;
— except for unscheduled ad hoc audits, ensure that personnel being visited will be informed about audit scope and objectives.

C.6.2 On-site activities
— avoid any unnecessary disturbance of the operational processes;
— ensure that the audit team is using PPE properly;
— schedule communication to minimize disruption;
— adapt size of the audit team and the number of guides and observers in accordance with the audit scope to avoid interference of the operational processes as far as practicable;
do not touch or manipulate any equipment, unless explicitly permitted, even when competent and/or licensed;

if an incident occurs during the on-site visit, agree with the auditee on continuation or interruption (rescheduling) of the audit;

if taking pictures, ask for authorisation from management in advance and consider security and confidentiality matters and avoid taking photograph of individual persons without their permission;

if taking copies of documents of any kind, ask for permission in advance and consider confidentiality and security matters;

when taking notes, avoid collecting personal information unless required by the audit objectives and/or audit criteria.

C.7 Conducting interviews

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

- interviews should be held with persons from appropriate levels and functions performing activities or tasks within the scope of the audit;
- interviews should be conducted during the normal working hours and, where practical, at the normal workplace of the person being interviewed;
- attempting to put the person interviewed at ease prior to and during the interview;
- the reason for the interview and any note taking should be explained;
- interviews may be initiated by asking the persons to describe their work;
- questions that bias the answers (i.e. leading questions) should be used carefully;
- the results from the interview should be summarized and reviewed with the interviewed person;
- the interviewed persons should be thanked for their participation and cooperation.

C.8 Audit findings

C.8.1 Recording individual audit findings

For recording individual audit findings of conformity the following should be considered:

- follow-up of previous audit records and conclusions;
- requirements of audit clients;
- findings exceeding normal practice, to be used as motivator, or opportunity for improvement.

C.8.2 Recording non conformities

Records of non conformities should include:

- description of audit criteria requirement;
C.8.3 Dealing with findings related to multiple criteria

On 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/similar criteria of the other management systems.

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

- separate findings for each criterion; or
- a single finding, combining the references to multiple criteria.

Depending on the arrangements with the person responsible for managing the audit programme, the auditor may guide the auditee on how to respond to those findings.
Bibliography


[10] ISO/CD 30301, Information and documentation -- Management system for records -- Requirements

    www.iso.org/tc176/ISO9001AuditingPracticesGroup

---

1) to be published