INTERNATIONAL STANDARD

ISO 19011

Second edition
2011-11-15

Guidelines for auditing management systems

Lignes directrices pour l'audit des systèmes de management

Reference number
ISO 19011:2011(E)

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

Published in Switzerland

Contents

Foreword

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

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

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

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

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

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

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

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

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

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

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

— Clauses 5, 6 and 7 have been reorganized;

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

— the competence determination and evaluation process has been strengthened;

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

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

Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Guidelines for auditing management systems

1 Scope

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

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

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

2 Normative references

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

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

3.3
audit evidence

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

NOTE Audit evidence can be qualitative or quantitative.

[ISO 9000:2005, definition 3.9.4]

3.4
audit findings

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

NOTE 1 Audit findings indicate conformity or nonconformity.

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

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

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

3.5
audit conclusion

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

NOTE Adapted from ISO 9000:2005, definition 3.9.6.

3.6
audit client

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

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

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

3.7
auditee

organization being audited

[ISO 9000:2005, definition 3.9.8]

3.8
auditor

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

3.9
audit team

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

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

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

[ISO 9000:2005, definition 3.9.10]

3.10
technical expert

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

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

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

[ISO 9000:2005, definition 3.9.11]

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

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

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

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

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

NOTE Adapted from ISO 9000:2005, definition 3.9.2.

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

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

[ISO 9000:2005, definition 3.9.13]

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

[ISO 9000:2005, definition 3.9.12]

3.16
risk
effect of uncertainty on objectives

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

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

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

3.18
conformity
fulfilment of a requirement

[ISO 9000:2005, definition 3.6.1]

3.19
nonconformity
non-fulfilment of a requirement

[ISO 9000:2005, definition 3.6.2]

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

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

[ISO 9000:2005, definition 3.2.2]

4 Principles of auditing

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

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

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

Auditors and the person managing an audit programme should:

- perform their work with honesty, diligence, and responsibility;
- observe and comply with any applicable legal requirements;
- demonstrate their competence while performing their work;
- perform their work in an impartial manner, i.e. remain fair and unbiased in all their dealings;
- be sensitive to any influences that may be exerted on their judgement while carrying out an audit.

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

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

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

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

d) **Confidentiality:** security of information

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

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

Auditors should be independent of the activity being audited wherever practicable, and should in all cases act in a manner that is free from bias and conflict of interest. For internal audits, auditors should be independent from the operating managers of the function being audited. Auditors should maintain objectivity throughout the audit process to ensure that the audit findings and conclusions are based only on the audit evidence.

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

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

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

5 Managing an audit programme

5.1 General

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

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

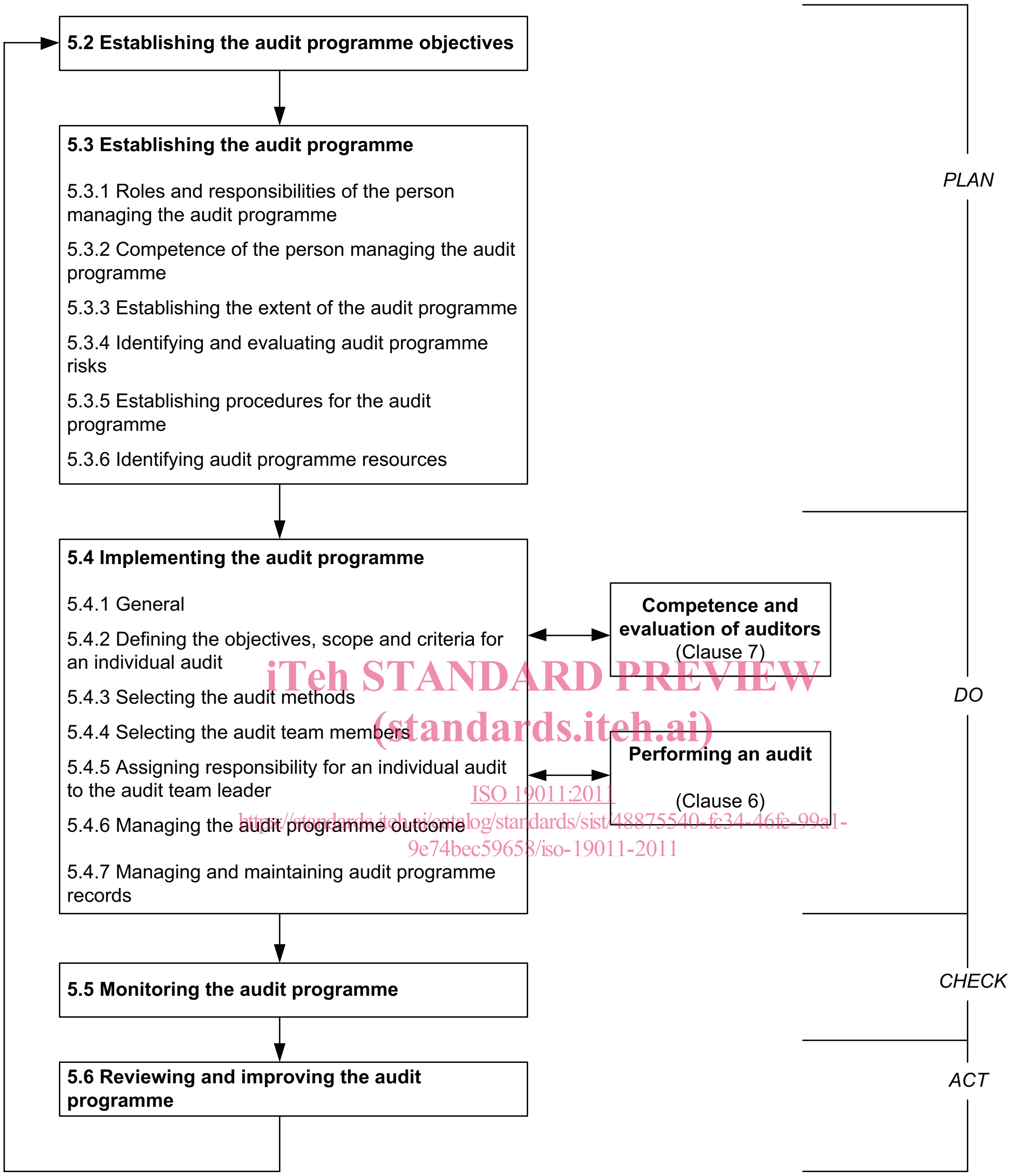
NOTE This concept is commonly known as risk-based auditing. This International Standard does not give further guidance on risk-based auditing.

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

- objectives for the audit programme and individual audits;
- extent/number/types/duration/locations/schedule of the audits;
- audit programme procedures;
- audit criteria;
- audit methods;
- selection of audit teams;
- necessary resources, including travel and accommodation;
- processes for handling confidentiality, information security, health and safety, and other similar matters.

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

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


5.2 Establishing the audit programme objectives
5.3 Establishing the audit programme
5.3.1 Roles and responsibilities of the person managing the audit programme
5.3.2 Competence of the person managing the audit programme
5.3.3 Establishing the extent of the audit programme
5.3.4 Identifying and evaluating audit programme risks
5.3.5 Establishing procedures for the audit programme
5.3.6 Identifying audit programme resources
5.4 Implementing the audit programme
5.4.1 General
5.4.2 Defining the objectives, scope and criteria for an individual audit
5.4.3 Selecting the audit methods
5.4.4 Selecting the audit team members
5.4.5 Assigning responsibility for an individual audit to the audit team leader
5.4.6 Managing the audit programme outcome
5.4.7 Managing and maintaining audit programme records
Competence and evaluation of auditors
(Clause 7)
Performing an audit
(Clause 6)
5.5 Monitoring the audit programme
5.6 Reviewing and improving the audit programme
PLAN
DO
CHECK
ACT

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

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

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

5.2 Establishing the audit programme objectives

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

These objectives can be based on consideration of the following:

a) management priorities;

b) commercial and other business intentions;

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

d) management system requirements;

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

f) need for supplier evaluation;

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

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

i) risks to the auditee;

j) results of previous audits;

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

Examples of audit programme objectives include the following:

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

5.3 Establishing the audit programme

5.3.1 Roles and responsibilities of the person managing the audit programme

The person managing the audit programme should:

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

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

5.3.2 Competence of the person managing the audit programme

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

- audit principles, procedures and methods;
- management system standards and reference documents;
- activities, products and processes of the auditee;
- applicable legal and other requirements relevant to the activities and products of the auditee;
- customers, suppliers and other interested parties of the auditee, where applicable.

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

5.3.3 Establishing the extent of the audit programme

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

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

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

- the objective, scope and duration of each audit and the number of audits to be conducted, including audit follow up, if applicable;
- the number, importance, complexity, similarity and locations of the activities to be audited;
- those factors influencing the effectiveness of the management system;
- applicable audit criteria, such as planned arrangements for the relevant management standards, legal and contractual requirements and other requirements to which the organization is committed;
- conclusions of previous internal or external audits;
- results of a previous audit programme review;
- language, cultural and social issues;
- the concerns of interested parties, such as customer complaints or non-compliance with legal requirements;
- significant changes to the auditee or its operations;
- availability of information and communication technologies to support audit activities, in particular the use of remote audit methods (see Clause B.1);
- the occurrence of internal and external events, such as product failures, information security leaks, health and safety incidents, criminal acts or environmental incidents.

5.3.4 Identifying and evaluating audit programme risks

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

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

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

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

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

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

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

5.3.5 Establishing procedures for the audit programme

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

— planning and scheduling audits considering audit programme risks;

— ensuring information security and confidentiality;

— assuring the competence of auditors and audit team leaders;

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

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

— conducting audit follow-up, if applicable;

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

— maintaining audit programme records;

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

5.3.6 Identifying audit programme resources

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

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

— audit methods;

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

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

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

— the availability of information and communication technologies.