INTERNATIONAL STANDARD

ISO/IEC 17021

Second edition
2011-02-01

Conformity assessment — Requirements for bodies providing audit and certification of management systems

Évaluation de la conformité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management

Reference number
ISO/IEC 17021:2011(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of conformity assessment, the ISO Committee on conformity assessment (CASCO) is responsible for the development of International Standards and Guides.

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

Draft International Standards 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/IEC 17021 was prepared by the *ISO Committee on conformity assessment* (CASCO).

It was circulated for voting to the national bodies of both ISO and IEC, and was approved by both organizations.

This second edition cancels and replaces the first edition (ISO/IEC 17021:2006), which has been revised to expand the scope. The first edition is provisionally retained for a period of one year until the systematic review of this second edition.

This International Standard has also been published in an unofficial, marked version indicating changes from the previous edition.

Introduction

Certification of a management system, such as a quality or environmental management system of an organization, is one means of providing assurance that the organization has implemented a system for the management of the relevant aspects of its activities, in line with its policy.

This International Standard specifies requirements for certification bodies. Observance of these requirements is intended to ensure that certification bodies operate management system certification in a competent, consistent and impartial manner, thereby facilitating the recognition of such bodies and the acceptance of their certifications on a national and international basis. This International Standard serves as a foundation for facilitating the recognition of management system certification in the interests of international trade.

Certification of a management system provides independent demonstration that the management system of the organization

a) conforms to specified requirements,

b) is capable of consistently achieving its stated policy and objectives, and

c) is effectively implemented.

Conformity assessment such as certification of a management system thereby provides value to the organization, its customers and interested parties.

In this International Standard, Clause 4 describes the principles on which credible certification is based. These principles help the reader to understand the essential nature of certification and they are a necessary prelude to Clauses 5 to 10. These principles underpin all the requirements in this International Standard, but such principles are not auditable requirements in their own right. Clause 10 describes two alternative ways of supporting and demonstrating the consistent achievement of the requirements in this International Standard through the establishment of a management system by the certification body.

This International Standard is intended for use by bodies that carry out audit and certification of management systems. It gives generic requirements for such certification bodies performing audit and certification in the field of quality, environmental and other forms of management systems. Such bodies are referred to as certification bodies. This wording should not be an obstacle to the use of this International Standard by bodies with other designations that undertake activities covered by the scope of this document.

Certification activities involve the audit of an organization's management system. The form of attestation of conformity of an organization's management system to a specific management system standard or other normative requirements is normally a certification document or a certificate.

The publication of this International Standard includes the text of ISO/IEC 17021:2006, including amendments to delete relevant references to ISO 19011, with new text adding specific requirements for third-party certification auditing and the management of competence of personnel involved in certification.

Specific market needs have already been identified, resulting from a lack of specific and recognized requirements for third-party auditors of management systems, such as quality management systems, environmental management systems or food safety management systems. The lack of requirements for auditor competence and the way in which these auditors are managed and deployed has been identified by key interested parties, including industry interested parties, as being a drawback.

This International Standard provides a set of requirements for management systems auditing at a generic level, aimed at providing a reliable determination of conformity to the applicable requirements for certification, conducted by a competent audit team, with adequate resources and following a consistent process, with the results reported in a consistent manner.

This International Standard is applicable to the auditing and certification of any type of management system. It is recognized that some of the requirements, and in particular those related to auditor competence, can be supplemented with additional criteria in order to achieve the expectations of the interested parties.

In this International Standard, the word “shall” indicates a requirement and the word “should” a recommendation.

Conformity assessment — Requirements for bodies providing audit and certification of management systems

1 Scope

This International Standard contains principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types (e.g. quality management systems or environmental management systems) and for bodies providing these activities. Certification bodies operating to this International Standard need not offer all types of management system certification.

Certification of management systems (named in this International Standard "certification") is a third-party conformity assessment activity (see ISO/IEC 17000:2004, 5.5). Bodies performing this activity are therefore third-party conformity assessment bodies (named in this International Standard "certification body/bodies").

NOTE 1 Certification of a management system is sometimes also called "registration", and certification bodies are sometimes called "registrars".

NOTE 2 A certification body can be non-governmental or governmental (with or without regulatory authority).

NOTE 3 This International Standard can be used as a criteria document for accreditation or peer assessment or other audit processes.

2 Normative references

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

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

ISO/IEC 17000:2004, *Conformity assessment — Vocabulary and general principles*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 9000, ISO/IEC 17000 and the following apply.

3.1
certified client
organization whose management system has been certified

3.2
impartiality
actual and perceived presence of objectivity

NOTE 1 Objectivity means that conflicts of interest do not exist or are resolved so as not to adversely influence subsequent activities of the certification body.

NOTE 2 Other terms that are useful in conveying the element of impartiality are: objectivity, independence, freedom from conflict of interests, freedom from bias, lack of prejudice, neutrality, fairness, open-mindedness, even-handedness, detachment, balance.

3.3
management system consultancy
participation in designing, implementing or maintaining a management system

EXAMPLES

a) preparing or producing manuals or procedures, and

b) giving specific advice, instructions or solutions towards the development and implementation of a management system.

NOTE Arranging training and participating as a trainer is not considered consultancy, provided that, where the course relates to management systems or auditing, it is confined to the provision of generic information that is freely available in the public domain; i.e. the trainer should not provide company-specific solutions.

3.4
third-party certification audit
audit carried out by an auditing organization independent of the client and the user, for the purpose of certifying the client's management system

NOTE 1 In the definitions which follow, the term “audit” has been used for simplicity to refer to third-party certification audit.

NOTE 2 Third-party certification audits include initial, surveillance, re-certification audits, and can also include special audits.

NOTE 3 Third-party certification audits are typically conducted by audit teams of those bodies providing certification of conformity to the requirements of management system standards.

NOTE 4 A joint audit is when two or more auditing organizations cooperate to audit a single client.

NOTE 5 A combined audit is when a client is being audited against the requirements of two or more management systems standards together.

NOTE 6 An integrated audit is when a client has integrated the application of requirements of two or more management systems standards into a single management system and is being audited against more than one standard.

3.5
client
organization whose management system is being audited for certification purposes

3.6
auditor
person who conducts an audit

3.7
competence
ability to apply knowledge and skills to achieve intended results

3.8
guide
person appointed by the client to assist the audit team

3.9
observer
person who accompanies the audit team but does not audit

3.10
technical area
area characterized by commonalities of processes relevant to a specific type of management system

4 Principles

4.1 General

4.1.1 These principles are the basis for the subsequent specific performance and descriptive requirements in this International Standard. This International Standard does not give specific requirements for all situations that can occur. These principles should be applied as guidance for the decisions that may need to be made for unanticipated situations. Principles are not requirements.

4.1.2 The overall aim of certification is to give confidence to all parties that a management system fulfils specified requirements. The value of certification is the degree of public confidence and trust that is established by an impartial and competent assessment by a third-party. Parties that have an interest in certification include, but are not limited to

a) the clients of the certification bodies,

b) the customers of the organizations whose management systems are certified,

c) governmental authorities,

d) non-governmental organizations, and

e) consumers and other members of the public.

4.1.3 Principles for inspiring confidence include

— impartiality,

— competence,

— responsibility,

— openness,

— confidentiality, and

— responsiveness to complaints.

4.2 Impartiality

4.2.1 Being impartial, and being perceived to be impartial, is necessary for a certification body to deliver certification that provides confidence.

4.2.2 It is recognized that the source of revenue for a certification body is its client paying for certification, and that this is a potential threat to impartiality.

4.2.3 To obtain and maintain confidence, it is essential that a certification body's decisions be based on objective evidence of conformity (or nonconformity) obtained by the certification body, and that its decisions are not influenced by other interests or by other parties.

4.2.4 Threats to impartiality include the following.

a) Self-interest threats: threats that arise from a person or body acting in their own interest. A concern related to certification, as a threat to impartiality, is financial self-interest.

b) Self-review threats: threats that arise from a person or body reviewing the work done by themselves. Auditing the management systems of a client to whom the certification body provided management systems consultancy would be a self-review threat.

c) Familiarity (or trust) threats: threats that arise from a person or body being too familiar with or trusting of another person instead of seeking audit evidence.

d) Intimidation threats: threats that arise from a person or body having a perception of being coerced openly or secretively, such as a threat to be replaced or reported to a supervisor.

4.3 Competence

Competence of the personnel supported by the management system of the certification body is necessary to deliver certification that provides confidence.

4.4 Responsibility

4.4.1 The client organization, not the certification body, has the responsibility for conformity with the requirements for certification.

4.4.2 The certification body has the responsibility to assess sufficient objective evidence upon which to base a certification decision. Based on audit conclusions, it makes a decision to grant certification if there is sufficient evidence of conformity, or not to grant certification if there is not sufficient evidence of conformity.

NOTE Any audit is based on sampling within an organization's management system and therefore is not a guarantee of 100 % conformity with requirements.

4.5 Openness

4.5.1 A certification body needs to provide public access to, or disclosure of, appropriate and timely information about its audit process and certification process, and about the certification status (i.e. the granting, extending, maintaining, renewing, suspending, reducing the scope of, or withdrawing of certification) of any organization, in order to gain confidence in the integrity and credibility of certification. Openness is a principle of access to, or disclosure of, appropriate information.

4.5.2 To gain or maintain confidence in certification, a certification body should provide appropriate access to, or disclosure of, non-confidential information about the conclusions of specific audits (e.g. audits in response to complaints) to specific interested parties.

4.6 Confidentiality

To gain the privileged access to information that is needed for the certification body to assess conformity to requirements for certification adequately, it is essential that a certification body keep confidential any proprietary information about a client.

4.7 Responsiveness to complaints

Parties that rely on certification expect to have complaints investigated and, if these are found to be valid, should have confidence that the complaints will be appropriately addressed and that a reasonable effort will be made to resolve the complaints. Effective responsiveness to complaints is an important means of protection for the certification body, its clients and other users of certification against errors, omissions or unreasonable behaviour. Confidence in certification activities is safeguarded when complaints are processed appropriately.

NOTE An appropriate balance between the principles of openness and confidentiality, including responsiveness to complaints, is necessary in order to demonstrate integrity and credibility to all users of certification.

5 General requirements

5.1 Legal and contractual matters

5.1.1 Legal responsibility

The certification body shall be a legal entity, or a defined part of a legal entity, such that it can be held legally responsible for all its certification activities. A governmental certification body is deemed to be a legal entity on the basis of its governmental status.

5.1.2 Certification agreement

The certification body shall have a legally enforceable agreement for the provision of certification activities to its client. In addition, where there are multiple offices of a certification body or multiple sites of a client, the certification body shall ensure there is a legally enforceable agreement between the certification body granting certification and issuing a certificate, and all the sites covered by the scope of the certification.

5.1.3 Responsibility for certification decisions

The certification body shall be responsible for, and shall retain authority for, its decisions relating to certification, including the granting, maintaining, renewing, extending, reducing, suspending and withdrawing of certification.

5.2 Management of impartiality

5.2.1 The certification body shall have top management commitment to impartiality in management system certification activities. The certification body shall have a publicly accessible statement that it understands the importance of impartiality in carrying out its management system certification activities, manages conflict of interest and ensures the objectivity of its management system certification activities.

5.2.2 The certification body shall identify, analyse and document the possibilities for conflict of interests arising from provision of certification including any conflicts arising from its relationships. Having relationships does not necessarily present a certification body with a conflict of interest. However, if any relationship creates a threat to impartiality, the certification body shall document and be able to demonstrate how it eliminates or minimizes such threats. This information shall be made available to the committee specified in 6.2. The demonstration shall cover all potential sources of conflict of interests that are identified, whether they arise from within the certification body or from the activities of other persons, bodies or organizations.

NOTE A relationship that threatens the impartiality of the certification body can be based on ownership, governance, management, personnel, shared resources, finances, contracts, marketing and payment of a sales commission or other inducement for the referral of new clients, etc.

5.2.3 When a relationship poses an unacceptable threat to impartiality (such as a wholly owned subsidiary of the certification body requesting certification from its parent), then certification shall not be provided.

NOTE See Note to 5.2.2.

5.2.4 A certification body shall not certify another certification body for its management system certification activities.

NOTE See Note to 5.2.2.

5.2.5 The certification body and any part of the same legal entity shall not offer or provide management system consultancy. This also applies to that part of government identified as the certification body.

5.2.6 The certification body and any part of the same legal entity shall not offer or provide internal audits to its certified clients. The certification body shall not certify a management system on which it provided internal audits within two years following the end of the internal audits. This also applies to that part of government identified as the certification body.

NOTE See Note to 5.2.2.

5.2.7 The certification body shall not certify a management system on which a client has received management system consultancy or internal audits, where the relationship between the consultancy organization and the certification body poses an unacceptable threat to the impartiality of the certification body.

NOTE 1 Allowing a minimum period of two years to elapse following the end of the management system consultancy is one way of reducing the threat to impartiality to an acceptable level.

NOTE 2 See Note to 5.2.2.

5.2.8 The certification body shall not outsource audits to a management system consultancy organization, as this poses an unacceptable threat to the impartiality of the certification body (see 7.5). This does not apply to individuals contracted as auditors covered in 7.3.

5.2.9 The certification body's activities shall not be marketed or offered as linked with the activities of an organization that provides management system consultancy. The certification body shall take action to correct inappropriate claims by any consultancy organization stating or implying that certification would be simpler, easier, faster or less expensive if the certification body were used. A certification body shall not state or imply that certification would be simpler, easier, faster or less expensive if a specified consultancy organization were used.

5.2.10 To ensure that there is no conflict of interests, personnel who have provided management system consultancy, including those acting in a managerial capacity, shall not be used by the certification body to take part in an audit or other certification activities if they have been involved in management system consultancy towards the client in question within two years following the end of the consultancy.

5.2.11 The certification body shall take action to respond to any threats to its impartiality arising from the actions of other persons, bodies or organizations.

5.2.12 All certification body personnel, either internal or external, or committees, who could influence the certification activities, shall act impartially and shall not allow commercial, financial or other pressures to compromise impartiality.

5.2.13 Certification bodies shall require personnel, internal and external, to reveal any situation known to them that may present them or the certification body with a conflict of interests. Certification bodies shall use this information as input to identifying threats to impartiality raised by the activities of such personnel or by the organizations that employ them, and shall not use such personnel, internal or external, unless they can demonstrate that there is no conflict of interests.

5.3 Liability and financing

5.3.1 The certification body shall be able to demonstrate that it has evaluated the risks arising from its certification activities and that it has adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations in each of its fields of activities and the geographic areas in which it operates.

5.3.2 The certification body shall evaluate its finances and sources of income and demonstrate to the committee specified in 6.2 that initially, and on an ongoing basis, commercial, financial or other pressures do not compromise its impartiality.

6 Structural requirements

6.1 Organizational structure and top management

6.1.1 The certification body shall document its organizational structure, showing duties, responsibilities and authorities of management and other certification personnel and any committees. When the certification body is a defined part of a legal entity, the structure shall include the line of authority and the relationship to other parts within the same legal entity.

6.1.2 The certification body shall identify the top management (board, group of persons, or person) having overall authority and responsibility for each of the following:

a) development of policies relating to the operation of the body;

b) supervision of the implementation of the policies and procedures;

c) supervision of the finances of the body;

d) development of management system certification services and schemes;

e) performance of audits and certification, and responsiveness to complaints;

f) decisions on certification;

g) delegation of authority to committees or individuals, as required, to undertake defined activities on its behalf;

h) contractual arrangements;

i) provision of adequate resources for certification activities.

6.1.3 The certification body shall have formal rules for the appointment, terms of reference and operation of any committees that are involved in the certification activities.

6.2 Committee for safeguarding impartiality

6.2.1 The structure of the certification body shall safeguard the impartiality of the activities of the certification body and shall provide for a committee to

a) assist in developing the policies relating to impartiality of its certification activities,

b) counteract any tendency on the part of a certification body to allow commercial or other considerations to prevent the consistent objective provision of certification activities,

c) advise on matters affecting confidence in certification, including openness and public perception, and

d) conduct a review, at least once annually, of the impartiality of the audit, certification and decision-making processes of the certification body.

Other tasks or duties may be assigned to the committee provided these additional tasks or duties do not compromise its essential role of ensuring impartiality.

6.2.2 The composition, terms of reference, duties, authorities, competence of members and responsibilities of this committee shall be formally documented and authorized by the top management of the certification body to ensure

a) representation of a balance of interests such that no single interest predominates (internal or external personnel of the certification body are considered to be a single interest, and shall not predominate),

b) access to all the information necessary to enable it to fulfil its functions (see also 5.2.2 and 5.3.2), and

c) that if the top management of the certification body does not respect the advice of this committee, the committee shall have the right to take independent action (e.g. informing authorities, accreditation bodies, stakeholders). In taking independent action, committees shall respect the confidentiality requirements of 8.5 relating to the client and certification body.

6.2.3 Although this committee cannot represent every interest, a certification body should identify and invite key interests. Such interests may include: clients of the certification body, customers of organizations whose management systems are certified, representatives of industry trade associations, representatives of governmental regulatory bodies or other governmental services, or representatives of non-governmental organizations, including consumer organizations.

7 Resource requirements

7.1 Competence of management and personnel

7.1.1 General considerations

The certification body shall have processes to ensure that personnel have appropriate knowledge relevant to the types of management systems and geographic areas in which it operates.

It shall determine the competence required for each technical area (as relevant for the specific certification scheme), and for each function in the certification activity.

It shall determine the means for the demonstration of competence prior to carrying out specific functions.

7.1.2 Determination of competence criteria

The certification body shall have a documented process for determining the competence criteria for personnel involved in the management and performance of audits and certification. Competence criteria shall be determined with regard to the requirements of each type of management system standard or specification, for each technical area, and for each function in the certification process. The output of the process shall be the documented criteria of required knowledge and skills necessary to effectively perform audit and certification tasks to be fulfilled to achieve the intended results. Annex A specifies the knowledge and skills that a certification body shall define for specific functions. Where additional specific competence criteria have been established for a specific certification scheme, e.g. ISO/TS 22003 (Food safety management systems), these shall be applied.

NOTE The term 'technical area' can be applied differently depending on the management system standard being considered. For any management system, the term is related to products and processes in the context of the scope of the management system standard. The technical areas can be defined by a specific certification scheme (e.g. ISO/TS 22003); or can be determined by the certification body. Examples of the application of the term 'technical area' for different types of management systems are as follows:

— For a quality management system standard, the term “technical area” is related to the processes needed to fulfil customer expectations and applicable statutory and regulatory requirements for the organization's products and services.

— For an environmental management system standard, the term “technical area” is related to the categories of activities, products and services related to the environmental aspects affecting air, water, land, natural resources, flora, fauna and humans.

— For a supply chain security management system standard, the term “technical area” is related to processes in the context of security risk of supplies, such as transportation, storage, and information.

— For an information security management system standard, the term “technical area” is related, among others, to the categories of information security technologies and practices, information and communication technology and business activities related to the selection of adequate and proportionate security controls that protect information assets.

7.1.3 Evaluation processes

The certification body shall have documented processes for the initial competence evaluation, and on-going monitoring of competence and performance of all personnel involved in the management and performance of audits and certification, applying the determined competence criteria. The certification body shall demonstrate that its evaluation methods are effective. The output from these processes shall be to identify personnel who have demonstrated the level of competence required for the different functions of the audit and certification process.

NOTE A number of evaluation methods that can be used to evaluate knowledge and skills are described in Annex B.

7.1.4 Other considerations

7.1.4.1 In determining the competence requirements for its personnel performing certification, the certification body shall address the functions undertaken by management and administrative personnel in addition to those directly performing audit and certification activities.

7.1.4.2 The certification body shall have access to the necessary technical expertise for advice on matters directly relating to certification for technical areas, types of management system and geographic areas in which the certification body operates. Such advice may be provided externally or by certification body personnel.

7.2 Personnel involved in the certification activities

7.2.1 The certification body shall have, as part of its own organization, personnel having sufficient competence for managing the type and range of audit programmes and other certification work performed.

7.2.2 The certification body shall employ, or have access to, a sufficient number of auditors, including audit team leaders, and technical experts to cover all of its activities and to handle the volume of audit work performed.

7.2.3 The certification body shall make clear to each person concerned their duties, responsibilities and authorities.

7.2.4 The certification body shall have defined processes for selecting, training, formally authorizing auditors and for selecting technical experts used in the certification activity. The initial competence evaluation of an auditor shall include the ability to apply required knowledge and skills during audits, as determined by a competent evaluator observing the auditor conducting an audit.

NOTE During the selection and training process described above desired personal behaviours can be considered. These are characteristics that affect an individual's ability to perform specific functions. Therefore, knowledge about the behaviours of individuals enables a certification body to take advantage of their strengths and to minimize the impact of their weaknesses. Desired personal behaviours that are important for personnel involved in certification activities are described in Annex D.

7.2.5 The certification body shall have a process to achieve and demonstrate effective auditing, including the use of auditors and audit team leaders possessing generic auditing skills and knowledge, as well as skills and knowledge appropriate for auditing in specific technical areas.

7.2.6 The certification body shall ensure that auditors (and, where needed, technical experts) are knowledgeable of its audit processes, certification requirements and other relevant requirements. The certification body shall give auditors and technical experts access to an up-to-date set of documented procedures giving audit instructions and all relevant information on the certification activities.

7.2.7 The certification body shall use auditors and technical experts only for those certification activities where they have demonstrated competence.

NOTE Assignment of auditors and technical experts to teams for specific audits is addressed in 9.1.3.

7.2.8 The certification body shall identify training needs and shall offer or provide access to specific training to ensure its auditors, technical experts and other personnel involved in certification activities are competent for the functions they perform.

7.2.9 The group or individual that takes the decision on granting, maintaining, renewing, extending, reducing, suspending or withdrawing certification shall understand the applicable standard and certification requirements, and shall have demonstrated competence to evaluate the audit processes and related recommendations of the audit team.

7.2.10 The certification body shall ensure the satisfactory performance of all personnel involved in the audit and certification activities. There shall be documented procedures and criteria for monitoring and measurement of the performance of all persons involved, based on the frequency of their usage and the level of risk linked to their activities. In particular, the certification body shall review the competence of its personnel in the light of their performance in order to identify training needs.

7.2.11 The documented monitoring procedures for auditors shall include a combination of on-site observation, review of audit reports and feedback from clients or from the market and shall be defined in documented requirements. This monitoring shall be designed in such a way as to minimize disturbance to the normal processes of certification, especially from the client's viewpoint.

7.2.12 The certification body shall periodically observe the performance of each auditor on-site. The frequency of on-site observations shall be based on need determined from all monitoring information available.

7.3 Use of individual external auditors and external technical experts

The certification body shall require external auditors and external technical experts to have a written agreement by which they commit themselves to comply with applicable policies and procedures as defined by the certification body. The agreement shall address aspects relating to confidentiality and to independence from commercial and other interests, and shall require the external auditors and external technical experts to notify the certification body of any existing or prior association with any organization they may be assigned to audit.

NOTE Use of individual auditors and technical experts under such agreements does not constitute outsourcing as described under 7.5.

7.4 Personnel records

The certification body shall maintain up-to-date personnel records, including relevant qualifications, training, experience, affiliations, professional status, competence and any relevant consultancy services that may have been provided. This includes management and administrative personnel in addition to those performing certification activities.

7.5 Outsourcing

7.5.1 The certification body shall have a process in which it describes the conditions under which outsourcing (which is subcontracting to another organization to provide part of the certification activities on behalf of the certification body) may take place. The certification body shall have a legally enforceable agreement covering the arrangements, including confidentiality and conflict of interests, with each body that provides outsourced services.

NOTE 1 This can include outsourcing to other certification bodies. Use of auditors and technical experts under contract is addressed in 7.3.

NOTE 2 For the purposes of this International Standard, the terms “outsourcing” and “subcontracting” are considered to be synonyms.

7.5.2 Decisions for granting, maintaining, renewing, extending, reducing, suspending or withdrawing certification shall never be outsourced.

7.5.3 The certification body shall

a) take responsibility for all activities outsourced to another body,

b) ensure that the body that provides outsourced services, and the individuals that it uses, conform to requirements of the certification body and also to the applicable provisions of this International Standard, including competence, impartiality and confidentiality, and

c) ensure that the body that provides outsourced services, and the individuals that it uses, is not involved, either directly or through any other employer, with an organization to be audited, in such a way that impartiality could be compromised.

7.5.4 The certification body shall have documented procedures for the qualification and monitoring of all bodies that provide outsourced services used for certification activities, and shall ensure that records of the competence of auditors and technical experts are maintained.

8 Information requirements

8.1 Publicly accessible information

8.1.1 The certification body shall maintain and make publicly accessible, or provide upon request, information describing its audit processes and certification processes for granting, maintaining, extending, renewing, reducing, suspending or withdrawing certification, and about the certification activities, types of management systems and geographical areas in which it operates.

8.1.2 Information provided by the certification body to any client or to the marketplace, including advertising, shall be accurate and not misleading.

8.1.3 The certification body shall make publicly accessible information about certifications granted, suspended or withdrawn.

8.1.4 On request from any party, the certification body shall provide the means to confirm the validity of a given certification.

NOTE 1 If the total information is split between several sources (e.g. in printed or electronic form or a combination of both), a system ensuring traceability and absence of ambiguity between the sources can be implemented (e.g. unique numbering system, or hyperlinks on Internet).

NOTE 2 In exceptional cases, access to certain information can be limited on the request of the client (e.g. for security reasons).

8.2 Certification documents

8.2.1 The certification body shall provide certification documents to the certified client by any means it chooses.

8.2.2 The effective date on a certification document shall not be before the date of the certification decision.

8.2.3 The certification document(s) shall identify the following:

a) the name and geographic location of each client whose management system is certified (or the geographic location of the headquarters and any sites within the scope of a multi-site certification);

b) the dates of granting, extending or renewing certification;

c) the expiry date or recertification due date consistent with the recertification cycle;

d) a unique identification code;

e) the standard and/or other normative document, including issue number and/or revision, used for audit of the certified client;

f) the scope of certification with respect to product (including service), process, etc., as applicable at each site;

g) the name, address and certification mark of the certification body; other marks (e.g. accreditation symbol) may be used provided they are not misleading or ambiguous;

h) any other information required by the standard and/or other normative document used for certification;

i) in the event of issuing any revised certification documents, a means to distinguish the revised documents from any prior obsolete documents.

8.3 Directory of certified clients

The certification body shall maintain and make publicly accessible, or provide upon request, by any means it chooses, a directory of valid certifications that as a minimum shall show the name, relevant normative document, scope and geographical location (e.g. city and country) for each certified client (or the geographic location of the headquarters and any sites within the scope of a multi-site certification).

NOTE The directory remains the sole property of the certification body.

8.4 Reference to certification and use of marks

8.4.1 A certification body shall have a policy governing any mark that it authorizes certified clients to use. This shall assure, among other things, traceability back to the certification body. There shall be no ambiguity, in the mark or accompanying text, as to what has been certified and which certification body has granted the certification. This mark shall not be used on a product or product packaging seen by the consumer or in any other way that may be interpreted as denoting product conformity.

NOTE ISO/IEC 17030 provides requirements for use of third-party marks.

8.4.2 A certification body shall not permit its marks to be applied to laboratory test, calibration or inspection reports, as such reports are deemed to be products in this context.

8.4.3 The certification body shall require that the client organization

a) conforms to the requirements of the certification body when making reference to its certification status in communication media such as the internet, brochures or advertising, or other documents,

b) does not make or permit any misleading statement regarding its certification,

c) does not use or permit the use of a certification document or any part thereof in a misleading manner,

d) upon suspension or withdrawal of its certification, discontinues its use of all advertising matter that contains a reference to certification, as directed by the certification body (see 9.6.3 and 9.6.6),

e) amends all advertising matter when the scope of certification has been reduced,

f) does not allow reference to its management system certification to be used in such a way as to imply that the certification body certifies a product (including service) or process,

g) does not imply that the certification applies to activities that are outside the scope of certification, and

h) does not use its certification in such a manner that would bring the certification body and/or certification system into disrepute and lose public trust.

8.4.4 The certification body shall exercise proper control of ownership and shall take action to deal with incorrect references to certification status or misleading use of certification documents, marks or audit reports.

NOTE Such action could include requests for correction and corrective action, suspension, withdrawal of certification, publication of the transgression and, if necessary, legal action.

8.5 Confidentiality

8.5.1 The certification body shall, through legally enforceable agreements, have a policy and arrangements to safeguard the confidentiality of the information obtained or created during the performance of certification activities at all levels of its structure, including committees and external bodies or individuals acting on its behalf.

8.5.2 The certification body shall inform the client, in advance, of the information it intends to place in the public domain. All other information, except for information that is made publicly accessible by the client, shall be considered confidential.

8.5.3 Except as required in this International Standard, information about a particular client or individual shall not be disclosed to a third party without the written consent of the client or individual concerned. Where the certification body is required by law to release confidential information to a third party, the client or individual concerned shall, unless regulated by law, be notified in advance of the information provided.

8.5.4 Information about the client from sources other than the client (e.g. complainant, regulators) shall be treated as confidential, consistent with the certification body's policy.

8.5.5 Personnel, including any committee members, contractors, personnel of external bodies or individuals acting on the certification body's behalf, shall keep confidential all information obtained or created during the performance of the certification body's activities.

8.5.6 The certification body shall have available and use equipment and facilities that ensure the secure handling of confidential information (e.g. documents, records).

8.5.7 When confidential information is made available to other bodies (e.g. accreditation body, agreement group of a peer assessment scheme), the certification body shall inform its client of this action.

8.6 Information exchange between a certification body and its clients

8.6.1 Information on the certification activity and requirements

The certification body shall provide and update clients on the following:

a) a detailed description of the initial and continuing certification activity, including the application, initial audits, surveillance audits, and the process for granting, maintaining, reducing, extending, suspending, withdrawing certification and recertification;

b) the normative requirements for certification;

c) information about the fees for application, initial certification and continuing certification;

d) the certification body's requirements for prospective clients to

1) comply with certification requirements,

2) make all necessary arrangements for the conduct of the audits, including provision for examining documentation and the access to all processes and areas, records and personnel for the purposes of initial certification, surveillance, recertification and resolution of complaints, and

3) make provisions, where applicable, to accommodate the presence of observers (e.g. accreditation auditors or trainee auditors);

e) documents describing the rights and duties of certified clients, including requirements, when making reference to its certification in communication of any kind in line with the requirements in 8.4;

f) information on procedures for handling complaints and appeals.

8.6.2 Notice of changes by a certification body

The certification body shall give its certified clients due notice of any changes to its requirements for certification. The certification body shall verify that each certified client complies with the new requirements.

NOTE Contractual arrangements with certified clients could be necessary to ensure implementation of these requirements. A model of a license agreement for the use of certification, including the aspects related to a notice of changes, as far as applicable, is found in Annex E of ISO/IEC Guide 28:2004.

8.6.3 Notice of changes by a client

The certification body shall have legally enforceable arrangements to ensure that the certified client informs the certification body, without delay, of matters that may affect the capability of the management system to continue to fulfil the requirements of the standard used for certification. These include, for example, changes relating to

a) the legal, commercial, organizational status or ownership,

b) organization and management (e.g. key managerial, decision-making or technical staff),

c) contact address and sites,

d) scope of operations under the certified management system, and

e) major changes to the management system and processes.

NOTE A model of license agreement for the use of certification, including the aspects related to a notice of changes, as far as applicable, is found in Annex E of ISO/IEC Guide 28:2004.

9 Process requirements

9.1 General requirements

9.1.1 Audit programme

9.1.1.1 An audit programme for the full certification cycle shall be developed to clearly identify the audit activity(ies) required to demonstrate that the client's management system fulfils the requirements for certification to the selected standard(s) or other normative document(s).

9.1.1.2 The audit programme shall include a two-stage initial audit, surveillance audits in the first and second years, and a recertification audit in the third year prior to expiration of certification. The three-year certification

cycle begins with the certification or recertification decision. The determination of the audit programme and any subsequent adjustments shall consider the size of the client organization, the scope and complexity of its management system, products and processes as well as demonstrated level of management system effectiveness and the results of any previous audits.

NOTE 1 Annex E is a flowchart of a typical third-party audit and certification process.

NOTE 2 Annex F lists additional items that can be considered when developing or revising an audit programme.

9.1.1.3 Where a certification body is taking account of certification or other audits already granted to the client, it shall collect sufficient, verifiable information to justify and record any adjustments to the audit programme.

9.1.2 Audit plan

9.1.2.1 General

The certification body shall ensure that an audit plan is established for each audit identified in the audit programme to provide the basis for agreement regarding the conduct and scheduling of the audit activities. This audit plan shall be based on documented requirements of the certification body.

9.1.2.2 Determining audit objectives, scope and criteria

9.1.2.2.1 The audit objectives shall be determined by the certification body. The audit scope and criteria, including any changes, shall be established by the certification body after discussion with the client.

9.1.2.2.2 The audit objectives shall describe what is to be accomplished by the audit and shall include the following:

a) determination of the conformity of the client's management system, or parts of it, with audit criteria;

b) evaluation of the ability of the management system to ensure the client organization meets applicable statutory, regulatory and contractual requirements;

NOTE A management system certification audit is not a legal compliance audit.

c) evaluation of the effectiveness of the management system to ensure the client organization is continually meeting its specified objectives;

d) as applicable, identification of areas for potential improvement of the management system.

9.1.2.2.3 The audit scope shall describe the extent and boundaries of the audit, such as physical locations, organizational units, activities and processes to be audited. Where the initial or re-certification process consists of more than one audit (e.g. covering different locations), the scope of an individual audit may not cover the full certification scope, but the totality of audits shall be consistent with the scope in the certification document.

NOTE Annex F lists additional items that can be considered when preparing or revising the audit scope.

9.1.2.2.4 The audit criteria shall be used as a reference against which conformity is determined, and shall include:

— the requirements of a defined normative document on management systems;

— the defined processes and documentation of the management system developed by the client.

9.1.2.3 Preparing the audit plan

The audit plan shall be appropriate to the objectives and the scope of the audit. The audit plan shall at least include or refer to the following:

a) the audit objectives;

b) the audit criteria;

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

d) the dates and sites where the on-site audit activities are to be conducted, including visits to temporary sites, as appropriate;

e) the expected time and duration of on-site audit activities;

f) the roles and responsibilities of the audit team members and accompanying persons.

NOTE 1 The audit plan information can be contained in more than one document.

NOTE 2 Annex F lists additional items that can be considered when preparing or revising the audit plan.

9.1.3 Audit team selection and assignments

9.1.3.1 The certification body shall have a process for selecting and appointing the audit team, including the audit team leader, taking into account the competence needed to achieve the objectives of the audit. If there is only one auditor, the auditor shall have the competence to perform the duties of an audit team leader applicable for that audit.

9.1.3.2 In deciding the size and composition of the audit team, consideration shall be given to the following:

a) audit objectives, scope, criteria and estimated time of the audit;

b) whether the audit is a combined, integrated or joint audit;

c) the overall competence of the audit team needed to achieve the objectives of the audit;

d) certification requirements (including any applicable statutory, regulatory or contractual requirements);

e) language and culture;

f) whether the members of the audit team have previously audited the client's management system.

9.1.3.3 The necessary knowledge and skills of the audit team leader and auditors may be supplemented by technical experts, translators and interpreters who shall operate under the direction of an auditor. Where translators or interpreters are used, they are to be selected such that they do not unduly influence the audit.

NOTE The criteria for the selection of technical experts are determined on a case-by-case basis by the needs of the audit team and the scope of the audit.

9.1.3.4 Auditors-in-training may be included in the audit team as participants, provided an auditor is appointed as an evaluator. The evaluator shall be competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training.

9.1.3.5 The audit team leader, in consultation with the audit team, shall assign to each team member responsibility for auditing specific processes, functions, sites, areas or activities. Such assignments shall take into account the need for competence, and the effective and efficient use of the audit team, as well as different roles and responsibilities of auditors, auditors-in-training and technical experts. Changes to the work assignments may be made as the audit progresses to ensure achievement of the audit objectives.

9.1.4 Determining audit time

9.1.4.1 The certification body shall have documented procedures for determining audit time, and for each client the certification body shall determine the time needed to plan and accomplish a complete and effective audit of the client's management system. The audit time determined by the certification body, and the justification for the determination, shall be recorded. In determining the audit time, the certification body shall consider, among other things, the following aspects:

a) the requirements of the relevant management system standard;

b) size and complexity;

c) technological and regulatory context;

d) any outsourcing of any activities included in the scope of the management system;

e) the results of any prior audits;

f) number of sites and multi-site considerations;

g) the risks associated with the products, processes or activities of the organization;

h) when audits are combined, joint or integrated.

Where specific criteria have been established for a specific certification scheme, e.g. ISO/TS 22003 or ISO/IEC 27006, these shall be applied.

9.1.4.2 The time spent by any team member that is not assigned as an auditor (i.e. technical experts, translators, interpreters, observers and auditors-in-training) shall not count in the above established audit time.

NOTE The use of translators, interpreters can necessitate additional audit time.

9.1.5 Multi-site sampling

Where multi-site sampling is utilized for the audit of a client's management system covering the same activity in various locations, the certification body shall develop a sampling programme to ensure proper audit of the management system. The rationale for the sampling plan shall be documented for each client.

9.1.6 Communication of audit team tasks

The tasks given to the audit team shall be defined and shall be made known to the client organization, and shall require the audit team to

a) examine and verify the structure, policies, processes, procedures, records and related documents of the client organization relevant to the management system,

b) determine that these meet all the requirements relevant to the intended scope of certification,

c) determine that the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the client's management system, and

d) communicate to the client, for its action, any inconsistencies between the client's policy, objectives and targets (consistent with the expectations in the relevant management system standard or other normative document) and the results.

9.1.7 Communication concerning audit team members

The certification body shall provide the name of and, when requested, make available background information on each member of the audit team, with sufficient time for the client organization to object to the appointment of any particular auditor or technical expert and for the certification body to reconstitute the team in response to any valid objection.

9.1.8 Communication of audit plan

The audit plan shall be communicated and the dates of the audit shall be agreed upon, in advance, with the client organization.

9.1.9 Conducting on-site audits

9.1.9.1 General

The certification body shall have a process for conducting on-site audits. This process shall include an opening meeting at the start of the audit and a closing meeting at the conclusion of the audit.

NOTE In addition to visiting physical location(s) (e.g. factory), “on-site” can include remote access to electronic site(s) that contain(s) information that is relevant to the audit of the management system.

9.1.9.2 Conducting the opening meeting

A formal opening meeting, where attendance shall be recorded, shall be held with the client's management and, where appropriate, those responsible for the functions or processes to be audited. The purpose of the opening meeting, which shall usually be conducted by the audit team leader, is to provide a short explanation of how the audit activities will be undertaken and shall include the following elements. The degree of detail shall be consistent with the familiarity of the client with the audit process:

a) introduction of the participants, including an outline of their roles;

b) confirmation of the scope of certification;

c) confirmation of the audit plan (including type and scope of audit, objectives and criteria), any changes, and other relevant arrangements with the client, such as the date and time for the closing meeting, interim meetings between the audit team and the client's management;

d) confirmation of formal communication channels between the audit team and the client;

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

f) confirmation of matters relating to confidentiality;

g) confirmation of relevant work safety, emergency and security procedures for the audit team;

h) confirmation of the availability, roles and identities of any guides and observers;

i) the method of reporting, including any grading of audit findings;

j) information about the conditions under which the audit may be prematurely terminated;

k) confirmation that the audit team leader and audit team representing the certification body is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails;

l) confirmation of the status of findings of the previous review or audit, if applicable;

m) methods and procedures to be used to conduct the audit based on sampling;

n) confirmation of the language to be used during the audit;

o) confirmation that, during the audit, the client will be kept informed of audit progress and any concerns;

p) opportunity for the client to ask questions.

9.1.9.3 Communication during the audit

9.1.9.3.1 During the audit, the audit team shall periodically assess audit progress and exchange information. The audit team leader shall reassign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the client.

9.1.9.3.2 Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g. safety), the audit team leader shall report this to the client and, if possible, to the certification body 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. The audit team leader shall report the outcome of the action taken to the certification body.

9.1.9.3.3 The audit team leader shall review with the client any need for changes to the audit scope which becomes apparent as on-site auditing activities progress and report this to the certification body.

9.1.9.4 Observers and guides

9.1.9.4.1 Observers

The presence and justification of observers during an audit activity shall be agreed to by the certification body and client prior to the conduct of the audit. The audit team shall ensure that observers do not influence or interfere in the audit process or outcome of the audit.

NOTE Observers can be members of the client's organization, consultants, witnessing accreditation body personnel, regulators or other justified persons.

9.1.9.4.2 Guides

Each auditor shall be accompanied by a guide, unless otherwise agreed to by the audit team leader and the client. Guide(s) are assigned to the audit team to facilitate the audit. The audit team shall ensure that guides do not influence or interfere in the audit process or outcome of the audit.

NOTE The responsibilities of a guide can include:

a) establishing contacts and timing for interviews;

b) arranging visits to specific parts of the site or organization;

c) ensuring that rules concerning site safety and security procedures are known and respected by the audit team members;

d) witnessing the audit on behalf of the client;

e) providing clarification or information as requested by an auditor.

9.1.9.5 Collecting and verifying information

9.1.9.5.1 During the audit, information relevant to the audit objectives, scope and criteria (including information relating to interfaces between functions, activities and processes) shall be collected by appropriate sampling and verified to become audit evidence.

9.1.9.5.2 Methods to collect information shall include, but are not limited to:

a) interviews;

b) observation of processes and activities;

c) review of documentation and records.

9.1.9.6 Identifying and recording audit findings

9.1.9.6.1 Audit findings summarizing conformity and detailing nonconformity and its supporting audit evidence shall be recorded and reported to enable an informed certification decision to be made or the certification to be maintained.

9.1.9.6.2 Opportunities for improvement may be identified and recorded, unless prohibited by the requirements of a management system certification scheme. Audit findings, however, which are nonconformities in accordance with 9.1.15 b) and c) shall not be recorded as opportunities for improvement.

9.1.9.6.3 A finding of nonconformity shall be recorded against a specific requirement of the audit criteria, contain a clear statement of the nonconformity and identify in detail the objective evidence on which the nonconformity is based. Nonconformities shall be discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood. The auditor however shall refrain from suggesting the cause of nonconformities or their solution.

NOTE Nonconformities, consistent with the requirements of 9.1.15 b), can be classified as major, whereas other nonconformities [9.1.15 c)] can be classified as minor nonconformities.

9.1.9.6.4 The audit team leader shall attempt to resolve any diverging opinions between the audit team and the client concerning audit evidence or findings, and unresolved points shall be recorded.

9.1.9.7 Preparing audit conclusions

Prior to the closing meeting, the audit team shall:

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

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

c) identify any necessary follow-up actions;

d) confirm the appropriateness of the audit programme or identify any modification required (e.g. scope, audit time or dates, surveillance frequency, competence).

9.1.9.8 Conducting the closing meeting

9.1.9.8.1 A formal closing meeting, where attendance shall be recorded, shall be held with the client's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting, which shall normally be conducted by the audit team leader, is to present the audit conclusions, including the recommendation regarding certification. Any nonconformities shall be presented in such a manner that they are understood, and the timeframe for responding shall be agreed.

NOTE "Understood" does not necessarily mean that the nonconformities have been accepted by the client.

9.1.9.8.2 The closing meeting shall also include the following elements. The degree of detail shall be consistent with the familiarity of the client with the audit process:

a) advising the client that the audit evidence collected was based on a sample of the information; thereby introducing an element of uncertainty;

b) the method and timeframe of reporting, including any grading of audit findings;

c) the certification body's process for handling nonconformities including any consequences relating to the status of the client's certification;

d) the timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit;

e) the certification body's post audit activities;

f) information about the complaint handling and appeal processes.

9.1.9.8.3 The client shall be given opportunity for questions. Any diverging opinions regarding the audit findings or conclusions between the audit team and the client shall be discussed and resolved where possible. Any diverging opinions that are not resolved shall be recorded and referred to the certification body.

9.1.10 Audit report

9.1.10.1 The certification body shall provide a written report for each audit. The audit team may identify opportunities for improvement but shall not recommend specific solutions. Ownership of the audit report shall be maintained by the certification body.

9.1.10.2 The audit team leader shall ensure that the audit report is prepared and shall be responsible for its content. The audit report shall provide an accurate, concise and clear record of the audit to enable an informed certification decision to be made and shall include or refer to the following:

a) identification of the certification body;

b) the name and address of the client and the client's management representative;

c) the type of audit (e.g. initial, surveillance or recertification audit);

d) the audit criteria;

e) the audit objectives;

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

g) identification of the audit team leader, audit team members and any accompanying persons;

h) the dates and places where the audit activities (on site or offsite) were conducted;

i) audit findings, evidence and conclusions, consistent with the requirements of the type of audit;

j) any unresolved issues, if identified.

9.1.11 Cause analysis of nonconformities

The certification body shall require the client to analyse the cause and describe the specific correction and corrective actions taken, or planned to be taken, to eliminate detected nonconformities, within a defined time.

9.1.12 Effectiveness of corrections and corrective actions

The certification body shall review the corrections, identified causes and corrective actions submitted by the client to determine if these are acceptable. The certification body shall verify the effectiveness of any correction and corrective actions taken. The evidence obtained to support the resolution of nonconformities shall be recorded. The client shall be informed of the result of the review and verification.

NOTE Verification of effectiveness of correction and corrective action can be carried out based on a review of documentation provided by the client, or where necessary, through verification on-site.

9.1.13 Additional audits

The client shall be informed if an additional full audit, an additional limited audit, or documented evidence (to be confirmed during future surveillance audits) will be needed to verify effective correction and corrective actions.

9.1.14 Certification decision

The certification body shall ensure that the persons or committees that make the certification or recertification decisions are different from those who carried out the audits.

9.1.15 Actions prior to making a decision

The certification body shall confirm, prior to making a decision, that

a) the information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification;

b) it has reviewed, accepted and verified the effectiveness of correction and corrective actions, for all nonconformities that represent

   1) failure to fulfil one or more requirements of the management system standard, or

   2) a situation that raises significant doubt about the ability of the client's management system to achieve its intended outputs;

c) it has reviewed and accepted the client's planned correction and corrective action for any other nonconformities.

9.2 Initial audit and certification

9.2.1 Application

The certification body shall require an authorized representative of the applicant organization to provide the necessary information to enable it to establish the following:

a) the desired scope of the certification;

b) the general features of the applicant organization, including its name and the address(es) of its physical location(s), significant aspects of its process and operations, and any relevant legal obligations;

c) general information, relevant for the field of certification applied for, concerning the applicant organization, such as its activities, human and technical resources, functions and relationship in a larger corporation, if any;

d) information concerning all outsourced processes used by the organization that will affect conformity to requirements;

e) the standards or other requirements for which the applicant organization is seeking certification;

f) information concerning the use of consultancy relating to the management system.

9.2.2 Application review

9.2.2.1 Before proceeding with the audit, the certification body shall conduct a review of the application and supplementary information for certification to ensure that

a) the information about the applicant organization and its management system is sufficient for the conduct of the audit;

b) the requirements for certification are clearly defined and documented, and have been provided to the applicant organization;

c) any known difference in understanding between the certification body and the applicant organization is resolved;

d) the certification body has the competence and ability to perform the certification activity;

e) the scope of certification sought, the location(s) of the applicant organization's operations, time required to complete audits and any other points influencing the certification activity are taken into account (language, safety conditions, threats to impartiality, etc.);

f) records of the justification for the decision to undertake the audit are maintained.

9.2.2.2 Following the review of the application, the certification body shall either accept or decline an application for certification. When the certification body declines an application for certification as a result of the review of application, the reasons for declining an application shall be documented and made clear to the client.

NOTE When declining an application for certification, the certification body should be careful not to act in conflict with the principles set out in Clause 4.

9.2.2.3 Based on this review, the certification body shall determine the competences it needs to include in its audit team and for the certification decision.

9.2.2.4 The audit team shall be appointed and composed of auditors (and technical experts, as necessary) who, between them, have the totality of the competences identified by the certification body as set out in 9.2.2.3 for the certification of the applicant organization. The selection of the team shall be performed with reference to the designations of competence of auditors and technical experts made under 7.2.5, and may include the use of both internal and external human resources.

9.2.2.5 The individual(s) who will be conducting the certification decision shall be appointed to ensure appropriate competence is available (see 7.2.9).

9.2.3 Initial certification audit

The initial certification audit of a management system shall be conducted in two stages: stage 1 and stage 2.

9.2.3.1 Stage 1 audit

9.2.3.1.1 The stage 1 audit shall be performed to

a) audit the client's management system documentation;

b) evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for the stage 2 audit;

c) review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the management system;

d) collect necessary information regarding the scope of the management system, processes and location(s) of the client, and related statutory and regulatory aspects and compliance (e.g. quality, environmental, legal aspects of the client's operation, associated risks, etc.);

e) review the allocation of resources for stage 2 audit and agree with the client on the details of the stage 2 audit;

f) provide a focus for planning the stage 2 audit by gaining a sufficient understanding of the client's management system and site operations in the context of possible significant aspects;

g) evaluate if the internal audits and management review are being planned and performed, and that the level of implementation of the management system substantiates that the client is ready for the stage 2 audit.

For most management systems, it is recommended that at least part of the stage 1 audit be carried out at the client's premises in order to achieve the objectives stated above.

9.2.3.1.2 Stage 1 audit findings shall be documented and communicated to the client, including identification of any areas of concern that could be classified as nonconformity during the stage 2 audit.

9.2.3.1.3 In determining the interval between stage 1 and stage 2 audits, consideration shall be given to the needs of the client to resolve areas of concern identified during the stage 1 audit. The certification body may also need to revise its arrangements for stage 2.

9.2.3.2 Stage 2 audit

The purpose of the stage 2 audit is to evaluate the implementation, including effectiveness, of the client's management system. The stage 2 audit shall take place at the site(s) of the client. It shall include at least the following:

a) information and evidence about conformity to all requirements of the applicable management system standard or other normative document;

b) performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document);

c) the client's management system and performance as regards legal compliance;

d) operational control of the client's processes;

e) internal auditing and management review;

f) management responsibility for the client's policies;

g) links between the normative requirements, policy, performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document), any applicable legal requirements, responsibilities, competence of personnel, operations, procedures, performance data and internal audit findings and conclusions.

9.2.4 Initial certification audit conclusions

The audit team shall analyse all information and audit evidence gathered during the stage 1 and stage 2 audits to review the audit findings and agree on the audit conclusions.

9.2.5 Information for granting initial certification

9.2.5.1 The information provided by the audit team to the certification body for the certification decision shall include, as a minimum,

a) the audit reports,

b) comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client,

c) confirmation of the information provided to the certification body used in the application review (see 9.2.2), and

d) a recommendation whether or not to grant certification, together with any conditions or observations.

9.2.5.2 The certification body shall make the certification decision on the basis of an evaluation of the audit findings and conclusions and any other relevant information (e.g. public information, comments on the audit report from the client).

9.3 Surveillance activities

9.3.1 General

9.3.1.1 The certification body shall develop its surveillance activities so that representative areas and functions covered by the scope of the management system are monitored on a regular basis, and take into account changes to its certified client and its management system.

9.3.1.2 Surveillance activities shall include on-site audits assessing the certified client's management system's fulfilment of specified requirements with respect to the standard to which the certification is granted. Other surveillance activities may include

a) enquiries from the certification body to the certified client on aspects of certification,

b) reviewing any client's statements with respect to its operations (e.g. promotional material, website),

c) requests to the client to provide documents and records (on paper or electronic media), and

d) other means of monitoring the certified client's performance.

9.3.2 Surveillance audit

9.3.2.1 Surveillance audits are on-site audits, but are not necessarily full system audits, and shall be planned together with the other surveillance activities so that the certification body can maintain confidence that the certified management system continues to fulfil requirements between recertification audits. The surveillance audit programme shall include, at least

a) internal audits and management review,

b) a review of actions taken on nonconformities identified during the previous audit,

c) treatment of complaints,

d) effectiveness of the management system with regard to achieving the certified client's objectives,

e) progress of planned activities aimed at continual improvement,

f) continuing operational control,

g) review of any changes, and

h) use of marks and/or any other reference to certification.

9.3.2.2 Surveillance audits shall be conducted at least once a year. The date of the first surveillance audit following initial certification shall not be more than 12 months from the last day of the stage 2 audit.

9.3.3 Maintaining certification

The certification body shall maintain certification based on demonstration that the client continues to satisfy the requirements of the management system standard. It may maintain a client's certification based on a positive conclusion by the audit team leader without further independent review, provided

a) for any nonconformity or other situation that may lead to suspension or withdrawal of certification, the certification body has a system that requires the audit team leader to report to the certification body the need to initiate a review by appropriately competent personnel (see 7.2.9), different from those who carried out the audit, to determine whether certification can be maintained, and

b) competent personnel of the certification body monitor its surveillance activities, including monitoring the reporting by its auditors, to confirm that the certification activity is operating effectively.

9.4 Recertification

9.4.1 Recertification audit planning

9.4.1.1 A recertification audit shall be planned and conducted to evaluate the continued fulfilment of all of the requirements of the relevant management system standard or other normative document. The purpose of the recertification audit is to confirm the continued conformity and effectiveness of the management system as a whole, and its continued relevance and applicability for the scope of certification.

9.4.1.2 The recertification audit shall consider the performance of the management system over the period of certification, and include the review of previous surveillance audit reports.

9.4.1.3 Recertification audit activities may need to have a stage 1 audit in situations where there have been significant changes to the management system, the client, or the context in which the management system is operating (e.g. changes to legislation).

9.4.1.4 In the case of multiple sites or certification to multiple management system standards being provided by the certification body, the planning for the audit shall ensure adequate on-site audit coverage to provide confidence in the certification.

9.4.2 Recertification audit

9.4.2.1 The recertification audit shall include an on-site audit that addresses the following:

a) the effectiveness of the management system in its entirety in the light of internal and external changes and its continued relevance and applicability to the scope of certification;

b) demonstrated commitment to maintain the effectiveness and improvement of the management system in order to enhance overall performance;

c) whether the operation of the certified management system contributes to the achievement of the organization's policy and objectives.

9.4.2.2 When, during a recertification audit, instances of nonconformity or lack of evidence of conformity are identified, the certification body shall define time limits for correction and corrective actions to be implemented prior to the expiration of certification.

9.4.3 Information for granting recertification

The certification body shall make decisions on renewing certification based on the results of the recertification audit, as well as the results of the review of the system over the period of certification and complaints received from users of certification.

9.5 Special audits

9.5.1 Extensions to scope

The certification body shall, in response to an application for extension to the scope of a certification already granted, undertake a review of the application and determine any audit activities necessary to decide whether or not the extension may be granted. This may be conducted in conjunction with a surveillance audit.

9.5.2 Short-notice audits

It may be necessary for the certification body to conduct audits of certified clients at short notice to investigate complaints (see 9.8), or in response to changes (see 8.6.3), or as follow up on suspended clients (see 9.6). In such cases

a) the certification body shall describe and make known in advance to the certified clients (e.g. in documents as described in 8.6.1) the conditions under which these short notice visits are to be conducted, and

b) the certification body shall exercise additional care in the assignment of the audit team because of the lack of opportunity for the client to object to audit team members.

9.6 Suspending, withdrawing or reducing the scope of certification

9.6.1 The certification body shall have a policy and documented procedure(s) for suspension, withdrawal or reduction of the scope of certification, and shall specify the subsequent actions by the certification body.

9.6.2 The certification body shall suspend certification in cases when, for example,

— the client's certified management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system,

— the certified client does not allow surveillance or recertification audits to be conducted at the required frequencies, or

— the certified client has voluntarily requested a suspension.

9.6.3 Under suspension, the client's management system certification is temporarily invalid. The certification body shall have enforceable arrangements with its clients to ensure that in case of suspension the client refrains from further promotion of its certification. The certification body shall make the suspended status of the certification publicly accessible (see 8.1.3) and shall take any other measures it deems appropriate.

9.6.4 Failure to resolve the issues that have resulted in the suspension in a time established by the certification body shall result in withdrawal or reduction of the scope of certification.

NOTE In most cases the suspension would not exceed 6 months.

9.6.5 The certification body shall reduce the client's scope of certification to exclude the parts not meeting the requirements, when the client has persistently or seriously failed to meet the certification requirements for those parts of the scope of certification. Any such reduction shall be in line with the requirements of the standard used for certification.

9.6.6 The certification body shall have enforceable arrangements with the certified client concerning conditions of withdrawal [see 8.4.3.d)] ensuring upon notice of withdrawal of certification that the client discontinues its use of all advertising matter that contains any reference to a certified status.

9.6.7 Upon request by any party, the certification body shall correctly state the status of certification of a client's management system as being suspended, withdrawn or reduced.

9.7 Appeals

9.7.1 The certification body shall have a documented process to receive, evaluate and make decisions on appeals.

9.7.2 A description of the appeals-handling process shall be publicly accessible.

9.7.3 The certification body shall be responsible for all decisions at all levels of the appeals-handling process. The certification body shall ensure that the persons engaged in the appeals-handling process are different from those who carried out the audits and made the certification decisions.

9.7.4 Submission, investigation and decision on appeals shall not result in any discriminatory actions against the appellant.

9.7.5 The appeals-handling process shall include at least the following elements and methods:

a) an outline of the process for receiving, validating and investigating the appeal, and for deciding what actions are to be taken in response to it, taking into account the results of previous similar appeals;

b) tracking and recording appeals, including actions undertaken to resolve them;

c) ensuring that any appropriate correction and corrective action are taken.

9.7.6 The certification body shall acknowledge receipt of the appeal and shall provide the appellant with progress reports and the outcome.

9.7.7 The decision to be communicated to the appellant shall be made by, or reviewed and approved by, individual(s) not previously involved in the subject of the appeal.

9.7.8 The certification body shall give formal notice to the appellant of the end of the appeals-handling process.

9.8 Complaints

9.8.1 A description of the complaints-handling process shall be publicly accessible.

9.8.2 Upon receipt of a complaint, the certification body shall confirm whether the complaint relates to certification activities that it is responsible for and, if so, shall deal with it. If the complaint relates to a certified client, then examination of the complaint shall consider the effectiveness of the certified management system.

9.8.3 Any complaint about a certified client shall also be referred by the certification body to the certified client in question at an appropriate time.

9.8.4 The certification body shall have a documented process to receive, evaluate and make decisions on complaints. This process shall be subject to requirements for confidentiality, as it relates to the complainant and to the subject of the complaint.

9.8.5 The complaints-handling process shall include at least the following elements and methods:

a) an outline of the process for receiving, validating, investigating the complaint, and for deciding what actions are to be taken in response to it;

b) tracking and recording complaints, including actions undertaken in response to them;

c) ensuring that any appropriate correction and corrective action are taken.

NOTE ISO 10002 provides guidance for complaints handling.

9.8.6 The certification body receiving the complaint shall be responsible for gathering and verifying all necessary information to validate the complaint.

9.8.7 Whenever possible, the certification body shall acknowledge receipt of the complaint, and shall provide the complainant with progress reports and the outcome.

9.8.8 The decision to be communicated to the complainant shall be made by, or reviewed and approved by, individual(s) not previously involved in the subject of the complaint.

9.8.9 Whenever possible, the certification body shall give formal notice of the end of the complaints-handling process to the complainant.

9.8.10 The certification body shall determine, together with the client and the complainant, whether and, if so to what extent, the subject of the complaint and its resolution shall be made public.

9.9 Records of applicants and clients

9.9.1 The certification body shall maintain records on the audit and other certification activities for all clients, including all organizations that submitted applications, and all organizations audited, certified, or with certification suspended or withdrawn.

9.9.2 Records on certified clients shall include the following:

a) application information and initial, surveillance and recertification audit reports;

b) certification agreement;

c) justification of the methodology used for sampling;

d) justification for auditor time determination (see 9.1.4);

e) verification of correction and corrective actions;

f) records of complaints and appeals, and any subsequent correction or corrective actions;

g) committee deliberations and decisions, if applicable;

h) documentation of the certification decisions;

i) certification documents, including the scope of certification with respect to product, process or service, as applicable;

j) related records necessary to establish the credibility of the certification, such as evidence of the competence of auditors and technical experts.

NOTE Methodology of sampling includes the sampling employed to assess the specific management system and/or to select sites in the context of multi-site assessment.

9.9.3 The certification body shall keep the records on applicants and clients secure to ensure that the information is kept confidential. Records shall be transported, transmitted or transferred in a way that ensures that confidentiality is maintained.

9.9.4 The certification body shall have a documented policy and documented procedures on the retention of records. Records shall be retained for the duration of the current cycle plus one full certification cycle.

NOTE In some jurisdictions, the law stipulates that records need to be maintained for a longer time period.

10 Management system requirements for certification bodies

10.1 Options

The certification body shall establish and maintain a management system that is capable of supporting and demonstrating the consistent achievement of the requirements of this International Standard. In addition to meeting the requirements of Clauses 5 to 9, the certification body shall implement a management system in accordance with either

a) management system requirements in accordance with ISO 9001 (see 10.2), or

b) general management system requirements (see 10.3).

10.2 Option 1: Management system requirements in accordance with ISO 9001

10.2.1 General

The certification body shall establish and maintain a management system, in accordance with the requirements of ISO 9001, that is capable of supporting and demonstrating the consistent achievement of the requirements of this International Standard, amplified by 10.2.2 to 10.2.4.

10.2.2 Scope

For application of the requirements of ISO 9001, the scope of the management system shall include the design and development requirements for its certification services.

10.2.3 Customer focus

For application of the requirements of ISO 9001, when developing its management system, the certification body shall consider the credibility of certification and shall address the needs of all parties (as set out in 4.1.2) that rely upon its audit and certification services, not just its clients.

10.2.4 Management review

For application of the requirements of ISO 9001, the certification body shall include as input for management review, information on relevant appeals and complaints from users of certification activities.

10.3 Option 2: General management system requirements

10.3.1 General

The certification body shall establish, document, implement and maintain a management system that is capable of supporting and demonstrating the consistent achievement of the requirements of this International Standard.

The certification body's top management shall establish and document policies and objectives for its activities. The top management shall provide evidence of its commitment to the development and implementation of the management system in accordance with the requirements of this International Standard. The top management shall ensure that the policies are understood, implemented and maintained at all levels of the certification body's organization.

The certification body's top management shall appoint a member of management who, irrespective of other responsibilities, shall have responsibility and authority that include

a) ensuring that processes and procedures needed for the management system are established, implemented and maintained, and

b) reporting to top management on the performance of the management system and any need for improvement.

10.3.2 Management system manual

All applicable requirements of this International Standard shall be addressed either in a manual or in associated documents. The certification body shall ensure that the manual and relevant associated documents are accessible to all relevant personnel.

10.3.3 Control of documents

The certification body shall establish procedures to control the documents (internal and external) that relate to the fulfilment of this International Standard. The procedures shall define the controls needed to

a) approve documents for adequacy prior to issue,

b) review and update as necessary and re-approve documents,

c) ensure that changes and the current revision status of documents are identified,

d) ensure that relevant versions of applicable documents are available at points of use,

e) ensure that documents remain legible and readily identifiable,

f) ensure that documents of external origin are identified and their distribution controlled, and

g) prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.

NOTE Documentation can be in any form or type of medium.

10.3.4 Control of records

The certification body shall establish procedures to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of its records related to the fulfilment of this International Standard.

The certification body shall establish procedures for retaining records for a period consistent with its contractual and legal obligations. Access to these records shall be consistent with the confidentiality arrangements.

NOTE For requirements for records on certified clients, see also 9.9.

10.3.5 Management review

10.3.5.1 General

The certification body's top management shall establish procedures to review its management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness, including the stated policies and objectives related to the fulfilment of this International Standard. These reviews shall be conducted at least once a year.

10.3.5.2 Review inputs

The input to the management review shall include information related to

a) results of internal and external audits,

b) feedback from clients and interested parties related to the fulfilment of this International Standard,

c) feedback from the committee for safeguarding impartiality,

d) the status of preventive and corrective actions,

e) follow-up actions from previous management reviews,

f) the fulfilment of objectives,

g) changes that could affect the management system, and

h) appeals and complaints.

10.3.5.3 Review outputs

The outputs from the management review shall include decisions and actions related to

a) improvement of the effectiveness of the management system and its processes,

b) improvement of the certification services related to the fulfilment of this International Standard, and

c) resource needs.

10.3.6 Internal audits

10.3.6.1 The certification body shall establish procedures for internal audits to verify that it fulfils the requirements of this International Standard and that the management system is effectively implemented and maintained.

NOTE ISO 19011 provides guidelines for conducting internal audits.

10.3.6.2 An audit programme shall be planned, taking into consideration the importance of the processes and areas to be audited, as well as the results of previous audits.

10.3.6.3 Internal audits shall be performed at least once every 12 months. The frequency of internal audits may be reduced if the certification body can demonstrate that its management system continues to be effectively implemented according to this International Standard and has proven stability.

10.3.6.4 The certification body shall ensure that

a) internal audits are conducted by qualified personnel knowledgeable in certification, auditing and the requirements of this International Standard,

b) auditors do not audit their own work,

c) personnel responsible for the area audited are informed of the outcome of the audit,

d) any actions resulting from internal audits are taken in a timely and appropriate manner, and

e) any opportunities for improvement are identified.

10.3.7 Corrective actions

The certification body shall establish procedures for identification and management of nonconformities in its operations. The certification body shall also, where necessary, take actions to eliminate the causes of nonconformities in order to prevent recurrence. Corrective actions shall be appropriate to the impact of the problems encountered. The procedures shall define requirements for

a) identifying nonconformities (e.g. from complaints and internal audits),

b) determining the causes of nonconformity,

c) correcting nonconformities,

d) evaluating the need for actions to ensure that nonconformities do not recur,

e) determining and implementing in a timely manner, the actions needed,

f) recording the results of actions taken, and

g) reviewing the effectiveness of corrective actions.

10.3.8 Preventive actions

The certification body shall establish procedures for taking preventive actions to eliminate the causes of potential nonconformities. Preventive actions taken shall be appropriate to the probable impact of the potential problems. The procedures for preventive actions shall define requirements for

a) identifying potential nonconformities and their causes,

b) evaluating the need for action to prevent the occurrence of nonconformities,

c) determining and implementing the action needed,

d) recording the results of actions taken, and

e) reviewing the effectiveness of the preventive actions taken.

NOTE The procedures for corrective and preventive actions do not necessarily have to be separate.

Annex A
(normative)

Required knowledge and skills

The following table specifies the knowledge and skills that a certification body shall define for specific certification functions. **X** means the certification body shall define the criteria and depth of knowledge and skills. **X+** indicates a need for deeper knowledge and skills.

Table A.1 — Table of knowledge and skills

Certification functions / Knowledge and skills	Conducting the application review to determine audit team competence required, to select the audit team members, and to determine the audit time	Reviewing audit reports and making certification decisions	Auditing	Leading the audit team
Knowledge of business management practices			X	X
Knowledge of audit principles, practices and techniques		X	X+	X+
Knowledge of specific management system standards/normative documents	X	X	X+	X+
Knowledge of certification body's processes	X	X	X	X
Knowledge of client business sector	X	X	X+	X+
Knowledge of client products, processes and organization	X		X	X
Language skills appropriate to all levels within the client organization			X	X
Note-taking and report-writing skills			X	X
Presentation skills			X	X+
Interviewing skills			X	X
Audit-management skills			X	X+

For knowledge of client products, processes and organization, where a team is performing the task, the expertise needs to exist within that team or could be provided by a technical expert. Where any audit is conducted by a team, the level of skills required should be held within the team as a whole and not by every individual member of the team.

The team leader of a combined or integrated audit should have an in-depth knowledge of at least one of the standards and is required to have awareness of the other standards used for that particular audit.

NOTE Risk and complexity are other considerations when deciding the level of expertise needed for any of these functions.

Annex B
(informative)

Possible evaluation methods

IMPORTANT — This annex is informative and not intended to be applied as requirements.

B.1 General

This annex is intended to provide examples of evaluation methods as an aid to certification bodies.

Methods for evaluating individuals' competence can be grouped into five major categories: review of records, feedback, interviews, observations and examinations. These can be further subdivided. The following is a brief description of each method and its usefulness and limitations for evaluating knowledge and skills. It is unlikely that any one method on its own will confirm competence.

The (following) methods in B.2 to B.6 can provide useful information of knowledge and skills; they are more effective when they are designed to be used with specified competence criteria resulting from the competence determination process specified in 7.1.2 and 7.1.3.

This is followed by an example of a process flow for determining and maintaining competence in Annex C.

B.2 Review of records

Some records are indicators of knowledge, such as a résumé or curriculum vitae showing work experience, audit experience, education and training.

Some records are indicators of skills, such as audit reports, records of work experience, audit experience, education and training.

Such records alone are not likely to be sufficient evidence of competence.

Other records are direct evidence of demonstration of competence such as a report of a performance appraisal of an auditor conducting an audit.

B.3 Feedback

Direct feedback from past employers can be an indicator of knowledge and skills, but it is important to note that sometimes employers specifically exclude negative information.

Personal references can be an indicator of knowledge and skills. It is unlikely that a candidate will provide a personal reference that would provide negative information.

Feedback by peers can be an indicator of knowledge and skills. Such feedback can be influenced by the relationship between the peers.

Feedback from clients can be an indicator of knowledge and skills. For an auditor, the feedback can be influenced by the results of the audit.

Feedback alone is not satisfactory evidence of competence.