INTERNATIONAL STANDARD

ISO/IEC 17021-1

First edition
2015-06-15

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

Part 1: Requirements

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

Partie 1: Exigences

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

Reference number
ISO/IEC 17021-1:2015(E)

© ISO/IEC 2015

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

 © ISO/IEC 2015 – All rights reserved

Contents

Page

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

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, ISO and IEC develop joint ISO/IEC documents under the management of the ISO Committee on Conformity assessment (ISO/CASCO).

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

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

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

ISO/IEC 17021-1 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 first edition of ISO/IEC 17021-1 cancels and replaces ISO/IEC 17021:2011, which has been technically revised.

ISO/IEC 17021 consists of the following parts, under the general title *Conformity assessment — Requirements for bodies providing audit and certification of management systems*:

— *Part 1: Requirements*

— *Part 2: Competence requirements for auditing and certification of environmental management systems* [Technical Specification]

— *Part 3: Competence requirements for auditing and certification of quality management systems* [Technical Specification]

— *Part 4: Competence requirements for auditing and certification of event sustainability management systems* [Technical Specification]

— *Part 5: Competence requirements for auditing and certification of asset management systems* [Technical Specification]

— *Part 6: Competence requirements for auditing and certification of business continuity management systems* [Technical Specification]

— *Part 7: Competence requirements for auditing and certification of road traffic safety management systems* [Technical Specification]

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

Introduction

Certification of a management system, such as the environmental management system, quality management system or information security 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, products and services, in line with the organization's policy and the requirements of the respective international management system standard.

This part of ISO/IEC 17021 specifies requirements for bodies providing audit and certification of management systems. It gives generic requirements for such bodies performing audit and certification in the field of quality, the environment and other types of management systems. Such bodies are referred to as 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 part of ISO/IEC 17021 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;

c) is effectively implemented.

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

Clause 4 describes the principles on which credible certification is based. These principles help the user to understand the essential nature of certification and they are a necessary prelude to Clauses 5 to 10. These principles underpin the requirements in this part of ISO/IEC 17021, 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 part of ISO/IEC 17021 through the establishment of a management system by the certification body.

Certification activities are the individual activities that make up the entire certification process, from application review to termination of certification. Annex E provides an illustration of the way in which many of these activities can interact.

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 usually a certification document or a certificate.

This part of ISO/IEC 17021 is applicable to the auditing and certification of any type of management system. It is recognized that some of the requirements, 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 part of ISO/IEC 17021, the following verbal forms are used:

— "shall" indicates a requirement;

— "should" indicates a recommendation;

— "may" indicates a permission;

— "can" indicates a possibility or a capability.

Further details can be found in the ISO/IEC Directives, Part 2.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

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

Part 1: Requirements

1 Scope

This part of ISO/IEC 17021 contains principles and requirements for the competence, consistency and impartiality of bodies providing audit and certification of all types of management systems.

Certification bodies operating to this part of ISO/IEC 17021 do not need to offer all types of management system certification.

Certification of management systems is a third-party conformity assessment activity (see ISO/IEC 17000:2004, 5.5) and bodies performing this activity are therefore third-party conformity assessment bodies.

NOTE 1 Examples of management systems include environmental management systems, quality management systems and information security management systems.

NOTE 2 In this part of ISO/IEC 17021, certification of management systems is referred to as "certification" and third-party conformity assessment bodies are referred to as "certification bodies".

NOTE 3 A certification body can be non-governmental or governmental, with or without regulatory authority.

NOTE 4 This part of ISO/IEC 17021 can be used as a criteria document for accreditation, peer assessment or other audit processes.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

2 Normative references

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

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

ISO/IEC 17000, *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
presence of objectivity

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

© ISO/IEC 2015 – All rights reserved

Note 2 to entry: Other terms that are useful in conveying the element of impartiality include “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 establishing, implementing or maintaining a management system

EXAMPLE 1 Preparing or producing manuals or procedures.

EXAMPLE 2 Giving specific advice, instructions or solutions towards the development and implementation of a management system.

Note 1 to entry: 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; i.e. the trainer should not provide client-specific solutions.

Note 2 to entry: The provision of generic information, but not client specific solutions for the improvement of processes or systems, is not considered to be consultancy. Such information may include:

— explaining the meaning and intention of certification criteria;

— identifying improvement opportunities;

— explaining associated theories, methodologies, techniques or tools;

— sharing non-confidential information on related best practices;

— other management aspects that are not covered by the management system being audited.

3.4
certification audit
audit carried out by an auditing organization independent of the client and the parties that rely on certification, for the purpose of certifying the client’s management system

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

Note 2 to entry: Certification audits include initial, surveillance, re-certification audits, and can also include special audits.

Note 3 to entry: Certification audits are typically conducted by audit teams of those bodies providing certification of conformity to the requirements of management system standards.

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

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

Note 6 to entry: 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

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

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 and its intended results

Note 1 to entry: See Note to 7.1.2.

3.11
nonconformity
non-fulfilment of a requirement

3.12
major nonconformity
nonconformity (3.11) that affects the capability of the management system to achieve the intended results

Note 1 to entry: Nonconformities could be classified as major in the following circumstances:

— if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;

— a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

3.13
minor nonconformity
nonconformity (3.11) that does not affect the capability of the management system to achieve the intended results

3.14
technical expert
person who provides specific knowledge or expertise to the audit team

Note 1 to entry: Specific knowledge or expertise is that which relates to the organization, the process or activity to be audited.

3.15
certification scheme
conformity assessment system related to management systems to which the same specified requirements, specific rules and procedures apply

3.16
audit time
time needed to plan and accomplish a complete and effective audit of the client organization's management system

3.17
duration of management system certification audits
part of *audit time* (3.16) spent conducting audit activities from the opening meeting to the closing meeting, inclusive

Note 1 to entry: Audit activities normally include:

— conducting the opening meeting;

— performing document review while conducting the audit;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

— communicating during the audit;

— assigning roles and responsibilities of guides and observers;

— collecting and verifying information;

— generating audit findings;

— preparing audit conclusions;

— conducting the closing meeting.

4 Principles

4.1 General

4.1.1 The principles described in this clause provide the basis for the subsequent specific performance and descriptive requirements in this part of ISO/IEC 17021. This part of ISO/IEC 17021 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;

e) consumers and other members of the public.

4.1.3 Principles for inspiring confidence include:

— impartiality;

— competence;

— responsibility;

— openness;

— confidentiality;

— responsiveness to complaints;

— risk-based approach.

NOTE This part of ISO/IEC 17021 sets out the principles of certification in Clause 4; the corresponding principles related to auditing can be found in ISO 19011:2011, Clause 4.

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. It is important that all internal and external personnel are aware of the need for impartiality.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

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 may include but are not limited to the following.

a) Self-interest: 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 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 that arise from a person or body being too familiar with or trusting of another person instead of seeking audit evidence.

d) Intimidation: 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

4.3.1 Competence of the personnel of the certification body in all functions involved in certification activities is necessary to deliver certification that provides confidence.

4.3.2 The competence also needs to be supported by the management system of the certification body.

4.3.3 It is a key issue for the management of the certification body to have an implemented process for the establishment of competence criteria for the personnel involved in the audit and other certification activities and to perform evaluation against the criteria.

4.4 Responsibility

4.4.1 The certified client, and not the certification body, has the responsibility for consistently achieving the intended results of implementation of the management system standard and 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, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

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 does not disclose any confidential information.

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 these complaints will be appropriately addressed, and that a reasonable effort will be made by the certification body to resolve them. 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.

4.8 Risk-based approach

Certification bodies need to take into account the risks associated with providing competent, consistent and impartial certification. Risks may include, but are not limited to, those associated with:

— the objectives of the audit;

— the sampling used in the audit process;

— real and perceived impartiality;

— legal, regulatory and liability issues;

— the client organization being audited and its operating environment;

— impact of the audit on the client and its activities;

— health and safety of the audit teams;

— perception of interested parties;

— misleading statements by the certified client;

— use of marks.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

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 that 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.

 © ISO/IEC 2015 – All rights reserved

5.1.2 Certification agreement

The certification body shall have a legally enforceable agreement with each client for the provision of certification activities in accordance with the relevant requirements of this part of ISO/IEC 17021. 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 the client that covers all the sites within the scope of the certification.

NOTE An agreement can be achieved through multiple agreements that reference or otherwise link to one another.

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, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring following suspension, or withdrawing of certification.

5.2 Management of impartiality

5.2.1 Conformity assessment activities shall be undertaken impartially. The certification body shall be responsible for the impartiality of its conformity assessment activities and shall not allow commercial, financial or other pressures to compromise impartiality.

5.2.2 The certification body shall have top management commitment to impartiality in management system certification activities. The certification body shall have a policy 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.

5.2.3 The certification body shall have a process to identify, analyse, evaluate, treat, monitor, and document the risks related to conflict of interests arising from provision of certification including any conflicts arising from its relationships on an ongoing basis. Where there are any threats to impartiality, the certification body shall document and demonstrate how it eliminates or minimizes such threats and document any residual risk. The demonstration shall cover all potential threats that are identified, whether they arise from within the certification body or from the activities of other persons, bodies or organizations. 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.

Top management shall review any residual risk to determine if it is within the level of acceptable risk.

The risk assessment process shall include identification of and consultation with appropriate interested parties to advise on matters affecting impartiality including openness and public perception. The consultation with appropriate interested parties shall be balanced with no single interest predominating.

NOTE 1 Sources of threats to impartiality of the certification body can be based on ownership, governance, management, personnel, shared resources, finances, contracts, training, marketing and payment of a sales commission or other inducement for the referral of new clients, etc.

NOTE 2 Interested parties can include personnel and 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.

NOTE 3 One way of fulfilling the consultation requirement of this clause is by the use of a committee of these interested parties.

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

5.2.5 The certification body and any part of the same legal entity and any entity under the organizational control of the certification body [see 9.5.1.2, bullet b)] shall not offer or provide management system consultancy. This also applies to that part of government identified as the certification body.

NOTE This does not preclude the possibility of exchange of information (e.g. explanation of findings or clarification of requirements) between the certification body and its clients.

5.2.6 The carrying out of internal audits by the certification body and any part of the same legal entity to its certified clients is a significant threat to impartiality. Therefore, the certification body and any part of the same legal entity and any entity under the organizational control of the certification body [see 9.5.1.2, bullet b)] shall not offer or provide internal audits to its certified clients. A recognized mitigation of this threat is that the certification body shall not certify a management system on which it provided internal audits for a minimum of two years following the completion of the internal audits.

NOTE See Note 1 to 5.2.3.

5.2.7 Where a client has received management systems consultancy from a body that has a relationship with a certification body, this is a significant threat to impartiality. A recognized mitigation of this threat is that the certification body shall not certify the management system for a minimum of two years following the end of the consultancy.

NOTE See Note 1 to 5.2.3.

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 links or statements 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 In order 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. A recognized mitigation of this threat is that personnel shall not be used for a minimum of 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 can present them or the certification body with a conflict of interests. Certification bodies shall record and 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 interest.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

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 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, duties, responsibilities and authorities of management and other personnel involved in certification 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 Certification activities shall be structured and managed so as to safeguard impartiality.

6.1.3 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 and establishment of processes and procedures relating to its operations;

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

c) ensuring impartiality;

d) supervision of its finances;

e) development of management system certification services and schemes;

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

g) decisions on certification;

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

i) contractual arrangements;

j) provision of adequate resources for certification activities.

6.1.4 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 Operational control

6.2.1 The certification body shall have a process for the effective control of certification activities delivered by branch offices, partnerships, agents, franchisees, etc., irrespective of their legal status, relationship or geographical location. The certification body shall consider the risk that these activities pose to the competence, consistency and impartiality of the certification body.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

6.2.2 The certification body shall consider the appropriate level and method of control of activities undertaken including its processes, technical areas of certification bodies' operations, competence of personnel, lines of management control, reporting and remote access to operations including records.

7 Resource requirements

7.1 Competence of personnel

7.1.1 General considerations

The certification body shall have processes to ensure that personnel have appropriate knowledge and skills relevant to the types of management systems (e.g. environmental management systems, quality management systems, information security management systems) and geographic areas in which it operates.

7.1.2 Determination of competence criteria

The certification body shall have a process for determining the competence criteria for personnel involved in the management and performance of audits and other certification activities. 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 standard or certification scheme (e.g. ISO/IEC TS 17021-2, ISO/IEC TS 17021-3 or ISO/TS 22003), these shall be applied.

NOTE The term "technical area" is applied differently depending on the management system standard being considered. For any management system, the term is related to products, processes and services in the context of the scope of the management system standard. The technical area can be defined by a specific certification scheme (e.g. ISO/TS 22003) or can be determined by the certification body. It is used to cover a number of other terms such as "scopes", "categories", "sectors", etc., which are traditionally used in different management system disciplines.

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 other certification activities, 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. Competence shall be demonstrated prior to the individual taking the responsibility for the performance of their activities within the certification body.

NOTE 1 A number of evaluation methods that can be used to evaluate competence are described in Annex B.

NOTE 2 Annex C shows an example of a process flow for determining and maintaining competence.

7.1.4 Other considerations

The certification body shall have access to the necessary technical expertise for advice on matters directly relating to certification activities for all technical areas, types of management systems 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 sufficient, competent personnel for managing and supporting the type and range of audit programmes and other certification work performed.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

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 processes for selecting, training, formally authorizing auditors and for selecting and familiarizing 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 behaviour can be considered. These are characteristics that affect an individual's ability to perform specific functions. Therefore, knowledge about the behaviour of individuals enables a certification body to take advantage of their strengths and to minimize the impact of their weaknesses. Desired personal behaviour that is important for personnel involved in certification activities is 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 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.

7.2.8 The group or individual that takes the decision on granting, refusing, maintaining, renewing, suspending, restoring, or withdrawing certification, or on expanding or reducing the scope of certification, shall understand the applicable standard and certification requirements, and shall have demonstrated competence to evaluate the outcomes of the audit processes including related recommendations of the audit team.

7.2.9 The certification body shall ensure the satisfactory performance of all personnel involved in the audit and other certification activities. There shall be a documented process for monitoring competence and 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 and record the competence of its personnel in the light of their performance in order to identify training needs.

7.2.10 The certification body shall monitor each auditor considering each type of management system to which the auditor is deemed competent. The documented monitoring process for auditors shall include a combination of on-site evaluation, review of audit reports and feedback from clients or from the market. 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.

7.2.11 The certification body shall periodically evaluate the performance of each auditor on-site. The frequency of on-site evaluations 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 implement processes as defined by the certification body. The agreement shall address aspects relating to confidentiality and

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

impartiality and shall require the external auditors and external technical experts to notify the certification body of any existing or prior relationship with any organization they may be assigned to audit.

NOTE Use of an individual or employee of another organization individually contracted to serve as an external auditor or technical expert does not constitute outsourcing.

7.4 Personnel records

The certification body shall maintain up-to-date personnel records, including relevant qualifications, training, experience, affiliations, professional status and competence. 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 conflicts of interests, with each body that provides outsourced services.

7.5.2 Decisions for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification shall not 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 part of ISO/IEC 17021, including competence, impartiality and confidentiality;

c) ensure that the body that provides outsourced services, and the individuals that it uses, are 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 a process for the approval and monitoring of all bodies that provide outsourced services used for certification activities, and shall ensure that records of the competence of all personnel involved in certification activities are maintained.

NOTE 1 For 7.5.1 to 7.5.4, where the certification body engages individuals or employees of other organizations to provide additional resources or expertise, these individuals do not constitute outsourcing provided they are individually contracted to operate under the certification body's management system (see 7.3).

NOTE 2 For 7.5.1 to 7.5.4, the terms "outsourcing" and "subcontracting" are considered to be synonyms.

8 Information requirements

8.1 Public information

8.1.1 The certification body shall maintain (through publications, electronic media or other means), and make public, without request, in all the geographical areas in which it operates, information about

a) audit processes;

b) processes for granting, refusing, maintaining, renewing, suspending, restoring or withdrawing certification or expanding or reducing the scope of certification;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

c) types of management systems and certification schemes in which it operates;

d) the use of the certification body's name and certification mark or logo;

e) processes for handling requests for information, complaints and appeals;

f) policy on impartiality.

8.1.2 The certification body shall provide upon request information about:

a) geographical areas in which it operates;

b) the status of a given certification;

c) the name, related normative document, scope and geographical location (city and country) for a specific certified client.

NOTE 1 In exceptional cases, access to certain information can be limited on the request of the client (e.g. for security reasons).

NOTE 2 The certification body can also make the information in 8.1.2 public by any means it chooses without request, e.g. on its internet website.

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

8.2 Certification documents

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

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

a) the name and geographical location of each certified client (or the geographical location of the headquarters and any sites within the scope of a multi-site certification);

b) the effective date of granting, expanding or reducing the scope of certification, or renewing certification which shall not be before the date of the relevant certification decision;

NOTE The certification body can keep the original certification date on the certificate when a certificate lapses for a period of time provided that:

— the current certification cycle start and expiry date are clearly indicated;

— the last certification cycle expiry date be indicated along with the date of recertification audit.

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

d) a unique identification code;

e) the management system standard and/or other normative document, including indication of issue status (e.g. revision date or number) used for audit of the certified client;

f) the scope of certification with respect to the type of activities, products and services as applicable at each site without being misleading or ambiguous;

g) the name, address and certification mark of the certification body; other marks (e.g. accreditation symbol, client's logo) 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;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

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

8.3 Reference to certification and use of marks

8.3.1 A certification body shall have rules governing any management system certification mark that it authorizes certified clients to use. These rules shall ensure, 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 nor product packaging nor in any other way that may be interpreted as denoting product conformity.

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

8.3.2 A certification body shall not permit its marks to be applied by certified clients to laboratory test, calibration or inspection reports or certificates.

8.3.3 A certification body shall have rules governing the use of any statement on product packaging or in accompanying information that the certified client has a certified management system. Product packaging is considered as that which can be removed without the product disintegrating or being damaged. Accompanying information is considered as separately available or easily detachable. Type labels or identification plates are considered as part of the product. The statement shall in no way imply that the product, process or service is certified by this means. The statement shall include reference to:

— identification (e.g. brand or name) of the certified client;

— the type of management system (e.g. quality, environment) and the applicable standard;

— the certification body issuing the certificate.

8.3.4 The certification body shall through legally enforceable arrangements require that the certified client:

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 withdrawal of its certification, discontinues its use of all advertising matter that contains a reference to certification, as directed by the certification body (see 9.6.5);

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 and sites that are outside the scope of certification;

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.

8.3.5 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

8.4 Confidentiality

8.4.1 The certification body shall be responsible, through legally enforceable agreements, for the management of all 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.

8.4.2 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.

8.4.3 Except as required in this part of ISO/IEC 17021, information about a particular certified client or individual shall not be disclosed to a third party without the written consent of the certified client or individual concerned.

8.4.4 When the certification body is required by law or authorized by contractual arrangements (such as with the accreditation body) to release confidential information, the client or individual concerned shall, unless prohibited by law, be notified of the information provided.

8.4.5 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.

8.4.6 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 except as required by law.

8.4.7 The certification body shall have processes and where applicable equipment and facilities that ensure the secure handling of confidential information.

8.5 Information exchange between a certification body and its clients

8.5.1 Information on the certification activity and requirements

The certification body shall provide information 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, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification;

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 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;

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

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 8.3;

f) information on processes for handling complaints and appeals.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

8.5.2 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.

8.5.3 Notice of changes by a certified 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;

e) major changes to the management system and processes.

The certification body shall take action as appropriate.

9 Process requirements

9.1 Pre-certification activities

9.1.1 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) relevant details of the applicant organization as required by the specific certification scheme, including its name and the address(es) of its site(s), its processes and operations, human and technical resources, functions, relationships and any relevant legal obligations;

c) identification of outsourced processes used by the organization that will affect conformity to requirements;

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

e) whether consultancy relating to the management system to be certified has been provided and, if so, by whom.

9.1.2 Application review

9.1.2.1 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 to develop an audit programme (see 9.1.3);

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

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

d) the scope of certification sought, the site(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.).

9.1.2.2 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.

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

9.1.3 Audit programme

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

9.1.3.2 The audit programme for the initial certification shall include a two-stage initial audit, surveillance audits in the first and second years following the certification decision, and a recertification audit in the third year prior to expiration of certification. The first three-year certification cycle begins with the certification decision. Subsequent cycles begin with the recertification decision (see 9.6.3.2.3) The determination of the audit programme and any subsequent adjustments shall consider the size of the client, 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 provides a flowchart of a typical audit and certification process.

NOTE 2 The following list contains additional items that can be considered when developing or revising an audit programme, they might also need to be addressed when determining the audit scope and developing the audit plan:

— complaints received by the certification body about the client;

— combined, integrated or joint audit

— changes to the certification requirements;

— changes to legal requirements;

— changes to accreditation requirements;

— organizational performance data (e.g. defect levels, key performance indicators data);

— relevant interested parties' concerns.

NOTE 3 If specified by the industry specific certification scheme, the certification cycle can be different from three years.

9.1.3.3 Surveillance audits shall be conducted at least once a calendar year, except in recertification years. The date of the first surveillance audit following initial certification shall not be more than 12 months from the certification decision date.

NOTE It can be necessary to adjust the frequency of surveillance audits to accommodate factors such as seasons or management systems certification of a limited duration (e.g. temporary construction site).

9.1.3.4 Where the certification body is taking account of certification already granted to the client and to audits performed by another certification body, it shall obtain and retain sufficient evidence, such as reports and documentation on corrective actions, to any nonconformity. The documentation shall support

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

the fulfilling of the requirements in this part of ISO/IEC 17021. The certification body shall, based on the information obtained, justify and record any adjustments to the existing audit programme and follow up the implementation of corrective actions concerning previous nonconformities.

9.1.3.5 Where the client operates shifts, the activities that take place during shift working shall be considered when developing the audit programme and audit plans.

9.1.4 Determining audit time

9.1.4.1 The certification body shall have documented procedures for determining audit time. 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.

9.1.4.2 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) complexity of the client and its management system;

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) size and number of sites, their geographical locations and multi-site considerations;

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

h) whether audits are combined, joint or integrated.

NOTE 1 Time spent travelling to and from audited sites is not included in the calculation of the duration of the management system audit days.

NOTE 2 The certification body can use the guidelines established in ISO/IEC TS 17023 for determining the duration of management system audit when documenting these procedures.

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

9.1.4.3 The duration of the management system audit and its justification shall be recorded.

9.1.4.4 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 duration of the management system audit.

NOTE The use of translators and interpreters can necessitate additional time.

9.1.5 Multi-site sampling

Where multi-site sampling is used for the audit of a client's management system covering the same activity in various geographical 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. Sampling is not allowed for some specific certification schemes, and where specific criteria have been established for a specific certification scheme, e.g. ISO/TS 22003, these shall be applied.

NOTE Where there are multiple sites not covering the same activity sampling is not appropriate.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

9.1.6 Multiple management systems standards

When certification to multiple management system standards is being provided by the certification body, the planning for the audit shall ensure adequate on-site auditing to provide confidence in the certification.

9.2 Planning audits

9.2.1 Determining audit objectives, scope and criteria

9.2.1.1 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.

9.2.1.2 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) determination of the ability of the management system to ensure the client meets applicable statutory, regulatory and contractual requirements;

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

c) determination of the effectiveness of the management system to ensure the client can reasonably expect to achieving its specified objectives;

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

9.2.1.3 The audit scope shall describe the extent and boundaries of the audit, such as sites, 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 sites), 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.

9.2.1.4 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.

9.2.2 Audit team selection and assignments

9.2.2.1 General

9.2.2.1.1 The certification body shall have a process for selecting and appointing the audit team, including the audit team leader and technical experts as necessary, taking into account the competence needed to achieve the objectives of the audit and requirements for impartiality. 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. The audit team shall have the totality of the competences identified by the certification body as set out in 9.1.2.3 for the audit.

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

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

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

c) the overall competence of the audit team needed to achieve the objectives of the audit (see Table A.1);

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

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

e) language and culture.

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

9.2.2.1.3 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 shall 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.

9.2.2.1.4 Auditors-in-training may participate in the audit, 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.

9.2.2.1.5 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.

9.2.2.2 Observers, technical experts and guides

9.2.2.2.1 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 unduly 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.

9.2.2.2.2 Technical experts

The role of technical experts during an audit activity shall be agreed to by the certification body and client prior to the conduct of the audit. A technical expert shall not act as an auditor in the audit team. The technical experts shall be accompanied by an auditor.

NOTE The technical experts can provide advice to the audit team for the preparation, planning or audit.

9.2.2.2.3 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 1 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;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

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

NOTE 2 Where appropriate, the auditee can also act as the guide.

9.2.3 Audit plan

9.2.3.1 General

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

NOTE It is not expected that a certification body will develop an audit plan for each audit at the time that the audit programme is developed.

9.2.3.2 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 will be conducted, including visits to temporary sites and remote auditing activities, where appropriate;

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

f) the roles and responsibilities of the audit team members and accompanying persons, such as observers or interpreters.

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

9.2.3.3 Communication of audit team tasks

The tasks given to the audit team shall be defined, and require the audit team to:

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

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;

d) communicate to the client, for its action, any inconsistencies between the client's policy, objectives and targets.

9.2.3.4 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.

9.2.3.5 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 to object to the

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

appointment of any particular audit team member and for the certification body to reconstitute the team in response to any valid objection.

9.3 Initial certification

9.3.1 Initial certification audit

9.3.1.1 General

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

9.3.1.2 Stage 1

9.3.1.2.1 Planning shall ensure that the objectives of stage 1 can be met and the client shall be informed of any "on site" activities during stage 1.

NOTE Stage 1 does not require a formal audit plan (see 9.2.3).

9.3.1.2.2 The objectives of stage 1 are to:

a) review the client's management system documented information;

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

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) obtain necessary information regarding the scope of the management system, including:

- the client's site(s);
- processes and equipment used;
- levels of controls established (particularly in case of multisite clients);
- applicable statutory and regulatory requirements;

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

f) provide a focus for planning stage 2 by gaining a sufficient understanding of the client's management system and site operations in the context of the management system standard or other normative document;

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

NOTE If at least part of stage 1 is carried out at the client's premises, this can help to achieve the objectives stated above.

9.3.1.2.3 Documented conclusions with regard to fulfilment of the stage 1 objectives and the readiness for stage 2 shall be communicated to the client, including identification of any areas of concern that could be classified as a nonconformity during stage 2.

NOTE The stage 1 output does not need to meet the full requirements of a report (see 9.4.8).

9.3.1.2.4 In determining the interval between stage 1 and stage 2, consideration shall be given to the needs of the client to resolve areas of concern identified during stage 1. The certification body may also

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

need to revise its arrangements for stage 2. If any significant changes which would impact the management system occur, the certification body shall consider the need to repeat all or part of stage 1. The client shall be informed that the results of stage 1 may lead to postponement or cancellation of stage 2.

9.3.1.3 Stage 2

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

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

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 ability and its performance regarding meeting of applicable statutory, regulatory and contractual requirements;

d) operational control of the client's processes;

e) internal auditing and management review;

f) management responsibility for the client's policies.

9.3.1.4 Initial certification audit conclusions

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

9.4 Conducting audits

9.4.1 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.

Where any part of the audit is made by electronic means or where the site to be audited is virtual, the certification body shall ensure that such activities are conducted by personnel with appropriate competence. The evidence obtained during such an audit shall be sufficient to enable the auditor to take an informed decision on the conformity of the requirement in question.

NOTE "On-site" audits can include remote access to electronic site(s) that contain(s) information that is relevant to the audit of the management system. Consideration can also be given to the use of electronic means for conducting audits.

9.4.2 Conducting the opening meeting

A formal opening meeting, 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, usually conducted by the audit team leader, is to provide a short explanation of how the audit activities will be undertaken. The degree of detail shall be consistent with the familiarity of the client with the audit process and shall consider the following:

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

b) confirmation of the scope of certification;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

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.

9.4.3 Communication during the audit

9.4.3.1 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.

9.4.3.2 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.

9.4.3.3 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.

9.4.4 Obtaining and verifying information

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

9.4.4.2 Methods to obtain information shall include, but are not limited to:

a) interviews;

b) observation of processes and activities;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

c) review of documentation and records.

9.4.5 Identifying and recording audit findings

9.4.5.1 Audit findings summarizing conformity and detailing nonconformity shall be identified, classified and recorded to enable an informed certification decision to be made or the certification to be maintained.

9.4.5.2 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, shall not be recorded as opportunities for improvement.

9.4.5.3 A finding of nonconformity shall be recorded against a specific requirement, and shall contain a clear statement of the nonconformity, identifying 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.

9.4.5.4 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.

9.4.6 Preparing audit conclusions

Under the responsibility of the audit team leader and prior to the closing meeting, the audit team shall:

a) review the audit findings, and any other appropriate information obtained during the audit, against the audit objectives and audit criteria and classify the nonconformities;

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

c) agree any necessary follow-up actions;

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

9.4.7 Conducting the closing meeting

9.4.7.1 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, usually 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.

9.4.7.2 The closing meeting shall also include the following elements where 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 obtained 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;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

e) the certification body's post audit activities;

f) information about the complaint and appeal handling processes.

9.4.7.3 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.

9.4.8 Audit report

9.4.8.1 The certification body shall provide a written report for each audit to the client. 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.

9.4.8.2 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 representative;

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

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) any deviation from the audit plan and their reasons;

h) any significant issues impacting on the audit programme;

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

j) the dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted;

k) audit findings (see 9.4.5), reference to evidence and conclusions, consistent with the requirements of the type of audit;

l) significant changes, if any, that affect the management system of the client since the last audit took place;

m) any unresolved issues, if identified;

n) where applicable, whether the audit is combined, joint or integrated;

o) a disclaimer statement indicating that auditing is based on a sampling process of the available information;

p) recommendation from the audit team

q) the audited client is effectively controlling the use of the certification documents and marks, if applicable;

r) verification of effectiveness of taken corrective actions regarding previously identified nonconformities, if applicable.

9.4.8.3 The report shall also contain:

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

a) a statement on the conformity and the effectiveness of the management system together with a summary of the evidence relating to:

   — the capability of the management system to meet applicable requirements and expected outcomes;

   — the internal audit and management review process;

b) a conclusion on the appropriateness of the certification scope;

c) confirmation that the audit objectives have been fulfilled.

9.4.9 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.

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

NOTE Verification of effectiveness of correction and corrective action can be carried out based on a review of documented information provided by the client, or where necessary, through verification on-site. Usually this activity is done by a member of the audit team.

9.5 Certification decision

9.5.1 General

9.5.1.1 The certification body shall ensure that the persons or committees that make the decisions for granting or refusing certification, expanding or reducing the scope of certification, suspending or restoring certification, withdrawing certification or renewing certification are different from those who carried out the audits. The individual(s) appointed to conduct the certification decision shall have appropriate competence.

9.5.1.2 The person(s) [excluding members of committees (see 6.1.4)] assigned by the certification body to make a certification decision shall be employed by, or shall be under legally enforceable arrangement with either the certification body or an entity under the organizational control of the certification body. A certification body's organizational control shall be one of the following:

a) whole or majority ownership of another entity by the certification body;

b) majority participation by the certification body on the board of directors of another entity;

c) a documented authority by the certification body over another entity in a network of legal entities (in which the certification body resides), linked by ownership or board of director control.

NOTE For governmental certification bodies, other parts of the same government can be considered to be "linked by ownership" to the certification body.

9.5.1.3 The persons employed by, or under contract with, entities under organizational control shall fulfil the same requirements of this part of ISO/IEC 17021 as persons employed by, or under contract with, the certification body.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

9.5.1.4 The certification body shall record each certification decision including any additional information or clarification sought from the audit team or other sources.

9.5.2 Actions prior to making a decision

The certification body shall have a process to conduct an effective review prior to making a decision for granting certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification, including, that

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

b) for any major nonconformities, it has reviewed, accepted and verified the correction and corrective actions;

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

9.5.3 Information for granting initial certification

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

a) the audit report;

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 9.1.2);

d) confirmation that the audit objectives have been achieved;

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

9.5.3.2 If the certification body is not able to verify the implementation of corrections and corrective actions of any major nonconformity within 6 months after the last day of stage 2, the certification body shall conduct another stage 2 prior to recommending certification.

9.5.3.3 When a transfer of certification is envisaged from one certification body to another, the accepting certification body shall have a process for obtaining sufficient information in order to take a decision on certification.

NOTE Certification schemes can have specific rules regarding the transfer of certification.

9.5.4 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.

9.6 Maintaining certification

9.6.1 General

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

based on a positive conclusion by the audit team leader without further independent review and decision, provided that:

a) for any major 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 competent personnel (see 7.2.8), different from those who carried out the audit, to determine whether certification can be maintained;

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.

9.6.2 Surveillance activities

9.6.2.1 General

9.6.2.1.1 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.

9.6.2.1.2 Surveillance activities shall include on-site auditing of 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 certified client's statements with respect to its operations (e.g. promotional material, website);

c) requests to the certified client to provide documented information (on paper or electronic media);

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

9.6.2.2 Surveillance audit

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 client's certified management system continues to fulfil requirements between recertification audits. Each surveillance for the relevant management system standard shall include:

a) internal audits and management review;

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

c) complaints handling;

d) effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system (s);

e) progress of planned activities aimed at continual improvement;

f) continuing operational control;

g) review of any changes;

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

9.6.3 Recertification

9.6.3.1 Recertification audit planning

9.6.3.1.1 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. 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. This shall be planned and conducted in due time to enable for timely renewal before the certificate expiry date.

9.6.3.1.2 The recertification activity shall include the review of previous surveillance audit reports and consider the performance of the management system over the most recent certification cycle.

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

NOTE Such changes can occur at any time during the certification cycle and the certification body might need to perform a special audit (see 9.6.4), which might or might not be a two-stage audit.

9.6.3.2 Recertification audit

9.6.3.2.1 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) the effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system (s).

9.6.3.2.2 For any major nonconformity, the certification body shall define time limits for correction and corrective actions. These actions shall be implemented and verified prior to the expiration of certification.

9.6.3.2.3 When recertification activities are successfully completed prior to the expiry date of the existing certification, the expiry date of the new certification can be based on the expiry date of the existing certification. The issue date on a new certificate shall be on or after the recertification decision.

9.6.3.2.4 If the certification body has not completed the recertification audit or the certification body is unable to verify the implementation of corrections and corrective actions for any major nonconformity (see 9.5.2.1) prior to the expiry date of the certification, then recertification shall not be recommended and the validity of the certification shall not be extended. The client shall be informed and the consequences shall be explained.

9.6.3.2.5 Following expiration of certification, the certification body can restore certification within 6 months provided that the outstanding recertification activities are completed, otherwise at least a stage 2 shall be conducted. The effective date on the certificate shall be on or after the recertification decision and the expiry date shall be based on prior certification cycle.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

9.6.4 Special audits

9.6.4.1 Expanding scope

The certification body shall, in response to an application for expanding 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.

9.6.4.2 Short-notice audits

It may be necessary for the certification body to conduct audits of certified clients at short notice or unannounced to investigate complaints, or in response to changes, or as follow up on suspended clients. 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 8.5.1) the conditions under which such audits will be conducted;

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.

9.6.5 Suspending, withdrawing or reducing the scope of certification

9.6.5.1 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.

9.6.5.2 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;

— the certified client has voluntarily requested a suspension.

9.6.5.3 Under suspension, the client's management system certification is temporarily invalid.

9.6.5.4 The certification body shall restore the suspended certification if the issue that has resulted in the suspension has been resolved. 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 six months.

9.6.5.5 The certification body shall reduce the scope of certification to exclude the parts not meeting the requirements, when the certified 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.

9.7 Appeals

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

9.7.2 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.

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

9.7.4 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 need 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.

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

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

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 The certification body shall be responsible for all decisions at all levels of the complaints-handling process.

9.8.2 Submission, investigation and decision on complaints shall not result in any discriminatory actions against the complainant.

9.8.3 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.

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

9.8.5 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.

9.8.6 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 need 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

NOTE ISO 10002 provides guidance for complaints handling.

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

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

9.8.9 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.

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

9.8.11 The certification body shall determine, together with the certified 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 Client records

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 of sites, as appropriate;

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

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;

k) audit programmes.

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

9.9.4 The certification body shall have a documented policy and documented procedures on the retention of records. Records of certified clients and previously certified clients 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, document, implement and maintain a management system that is capable of supporting and demonstrating the consistent achievement of the requirements of this part of ISO/IEC 17021. In addition to meeting the requirements of Clauses 5 to 9, the certification body shall implement a management system in accordance with either:

a) general management system requirements (see 10.2); or

b) management system requirements in accordance with ISO 9001 (see 10.3).

10.2 Option A: General management system requirements

10.2.1 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 part of ISO/IEC 17021.

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 part of ISO/IEC 17021. 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 assign responsibility and authority for:

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

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

10.2.2 Management system manual

All applicable requirements of this part of ISO/IEC 17021 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.

10.2.3 Control of documents

The certification body shall establish procedures to control the documents (internal and external) that relate to the fulfilment of this part of ISO/IEC 17021. The procedures shall define the controls needed to:

a) approve documents for adequacy prior to issue;

b) review and update where 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;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

e) ensure that documents remain legible and readily identifiable;

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

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.

10.2.4 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 part of ISO/IEC 17021.

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.

10.2.5 Management review

10.2.5.1 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 part of ISO/IEC 17021. These reviews shall be conducted at least once a year.

10.2.5.2 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;

c) safeguarding impartiality;

d) the status of corrective actions;

e) the status of actions to address risks;

f) follow-up actions from previous management reviews;

g) the fulfilment of objectives;

h) changes that could affect the management system;

i) appeals and complaints.

10.2.5.3 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 part of ISO/IEC 17021;

c) resource needs;

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

d) revisions of the organization's policy and objectives.

10.2.6 Internal audits

10.2.6.1 The certification body shall establish procedures for internal audits to verify that it fulfils the requirements of this part of ISO/IEC 17021 and that the management system is effectively implemented and maintained.

NOTE ISO 19011 provides guidelines for conducting internal audits.

10.2.6.2 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.

10.2.6.3 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 part of ISO/IEC 17021 and has proven stability.

10.2.6.4 The certification body shall ensure that:

a) internal audits are conducted by competent personnel knowledgeable in certification, auditing and the requirements of this part of ISO/IEC 17021;

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;

e) any opportunities for improvement are identified.

10.2.7 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 valid 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;

g) reviewing the effectiveness of corrective actions.

10.3 Option B: Management system requirements in accordance with ISO 9001

10.3.1 General

The certification body shall establish and maintain a management system, in accordance with the requirements of ISO 9001, which is capable of supporting and demonstrating the consistent achievement of the requirements of this part of ISO/IEC 17021, amplified by 10.3.2 to 10.3.4.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

 © ISO/IEC 2015 – All rights reserved

10.3.2 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.

10.3.3 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.

10.3.4 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 and a review of impartiality.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

© ISO/IEC 2015 – All rights reserved

Annex A
(normative)

Required knowledge and skills

A.1 General

Table A.1 specifies the knowledge and skills that a certification body shall define for specific certification functions. "X" indicates that the certification body shall define the criteria and depth of knowledge and skills. The knowledge and skill requirements specified in Table A.1 are explained in more detail in the text following the table and are referenced by the number in parenthesis.

Table A.1 — Table of knowledge and skills

Knowledge and skills	Certification functions		
	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 and leading the audit team
Knowledge of business management practices			X (see A.2.1)
Knowledge of audit principles, practices and techniques		X (see A.3.1)	X (see A.2.2)
Knowledge of specific management system standards/normative documents	X (see A.4.1)	X (see A.3.2)	X (see A.2.3)
Knowledge of certification body's processes	X (see A.4.2)	X (see A.3.3)	X (see A.2.4)
Knowledge of client's business sector	X (see A.4.3)	X(see A.3.4)	X (see A.2.5)
Knowledge of client products, processes and organization	X (see A.4.4)		X (see A.2.6)
Language skills appropriate to all levels within the client organization			X (see A.2.7)
Note-taking and report-writing skills			X (see A.2.8)
Presentation skills			X (see A.2.9)
Interviewing skills			X (see A.2.10)
Audit-management skills			X (see A.2.11)
NOTE Risk and complexity are other considerations when deciding the level of expertise needed for any of these functions.			

IECNORM.COM : Click to view the full PDF of ISO/IEC 17021-1:2015

A.2 Competence requirements for management systems auditors

A.2.1 Knowledge of business management practices

Knowledge of general organization types, size, governance, structure and work place practices, information and data systems, documentation systems, and information technology.

© ISO/IEC 2015 – All rights reserved