INTERNATIONAL STANDARD

ISO 28003

First edition
2007-08-01

Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems

Systèmes de management de la sûreté pour la chaîne d'approvisionnement — Exigences pour les organismes effectuant l'audit et la certification des systèmes de management de la sûreté pour la chaîne d'approvisionnement

Reference number
ISO 28003:2007(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights.

ISO 28003 was prepared jointly by the ISO *Committee on conformity assessment* (ISO/CASCO) and ISO/TC 8, *Ships and marine technology*.

This first edition cancels and replaces ISO/PAS 28003:2006, which has been technically revised.

ISO 28003 encompasses the requirements from ISO/IEC 17021, *Conformity assessment — Requirements for bodies providing audit and certification of management systems.* When assessing security supply chain security management systems, a number of requirements need to be met which go beyond what is required for the assessment and certification of supply chain security management systems covering other operational aspects of organizations. To formulate these additional requirements, ISO/IEC 17021 has been amended or modified where needed.

Introduction

This International Standard is intended for use by bodies that carry out audit and certification of supply chain security management systems. Certification of supply chain security management systems is a third party conformity assessment activity (see clause 5.5 of ISO/IEC 17000:2004). Bodies performing this activity are therefore third party conformity assessment bodies, named 'certification body/bodies' in this International Standard. This wording should not be an obstacle to the use of this International Standard by bodies with other designations that undertake activities covered by the scope of this International Standard. Indeed, this International Standard will be usable by any body involved in the assessment of supply chain security management systems.

Certification of supply chain security management systems of an organization is one means of providing assurance that the organization has implemented a system for supply chain security management in line with its policy.

Certification of supply chain security management systems will be delivered by certification bodies accredited by a recognized body, such as IAF members.

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

Certification of a supply chain security management system provides independent verification that the supply chain security 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.

Certification of a supply chain security management system thereby provides value to the organization, its customers and interested parties.

This International Standard aims at being the basis for recognition of the competence of certification bodies in their provision of supply chain security management system certification. This International Standard can be used as the basis for recognition of the competence of certification bodies in their provision of supply chain security management system certification (such recognition may be in the form of notification, peer assessment, or direct recognition by regulatory authorities or industry consortia).

Observance of the requirements in this International Standard is intended to ensure that certification bodies operate supply chain security management system certification in a competent, consistent and reliable manner, thereby facilitating the recognition of such bodies and the acceptance of their certifications on a national and international basis. This International Standard will serve as a foundation for facilitating the recognition of supply chain security management system certification in the interests of international trade.

Certification activities involve the audit of an organization's supply chain security management system. The form of attestation of conformity of an organization's supply chain security management system to a specific standard (for example ISO 28000) or other specified requirements is normally a certification document or a certificate.

It is for the organization being certified to develop its own supply chain security management systems (including ISO 28000 supply chain security management system, other sets of specified supply chain security management system requirements, quality systems, environmental supply chain security management systems or occupational health and safety supply chain security management systems) and, other than where relevant legislative requirements specify to the contrary, it is for the organization to decide how the various components of these are to be arranged. The degree of integration between the various supply chain security management system components will vary from organization to organization. It is therefore appropriate for certification bodies that operate in accordance with this International Standard to take into account the culture and practices of their clients in respect of the integration of their supply chain security management system within the wider organization.

Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems

1 Scope

This International Standard contains principles and requirements for bodies providing the audit and certification of supply chain security management systems according to management system specifications and standards such as ISO 28000.

It defines the minimum requirements of a certification body and its associated auditors, recognizing the unique need for confidentiality when auditing and certifying/registering a client organization.

Requirements for supply chain security management systems can originate from a number of sources, and this International Standard has been developed to assist in the certification of supply chain security management systems that fulfil the requirements of ISO 28000, *Specification for security management systems for the supply chain*, and other supply chain security management system International Standards. The contents of this International Standard may also be used to support certification of supply chain security management systems that are based on other specified supply chain security management system requirements.

This International Standard

— provides harmonized guidance for the accreditation of certification bodies applying for ISO 28000 (or other specified supply chain security management system requirements) certification/registration;

— defines the rules applicable for the audit and certification of a supply chain security management system complying with the supply chain security management system standard's requirements (or other sets of specified supply chain security management system requirements);

— provides the customers with the necessary information and confidence about the way certification of their suppliers has been granted.

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

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

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

2 Normative references

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

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

ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

ISO 28000:—[1], *Specification for security management systems for the supply chain*

3 Terms and definitions

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

3.1
certified client
organization whose supply chain security management system has been certified/registered by a qualified third party

3.2
impartiality
actual and perceived presence of objectivity

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

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

3.3
management system consultancy and/or associated risk assessments
participation in designing, implementing or maintaining a supply chain security management system and in conducting risk assessments

EXAMPLES

a) preparing or producing manuals or procedures;

b) giving specific advice, instructions or solutions towards the development and implementation of a supply chain security management system;

c) conducting internal audits;

d) conducting risk assessment and analysis.

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

4 Principles for certification bodies

4.1 General

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

4.1.2 The overall aim of certification is to give confidence to all parties that a supply chain security management system, process or product (including services) fulfils specified requirements. The value of certification is the degree of public confidence and trust that is established in a management system, process

1) To be published.

or product (including services) after it has been impartially and competently assessed 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) nongovernmental organizations;

e) consumers and other members of the public.

4.1.3 Principles for inspiring confidence include:

a) impartiality,

b) competence,

c) responsibility,

d) openness,

e) confidentiality,

f) responsiveness to complaints.

4.2 Impartiality

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

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

4.2.3 To obtain and maintain confidence, a certification body has to be able to demonstrate that its decisions are based on objective evidence of conformity (or nonconformity) obtained by the certification body, and that its decisions are not influenced by other interests or by other parties.

4.2.4 Threats to impartiality include:

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

b) Self-review threats — threats that arise from a person or body reviewing the work done by themselves. Auditing the supply chain security management systems of a client to whom the certification body provided supply chain security management systems consultancy would be a self-review threat and therefore is not acceptable.

c) Familiarity (or trust) threats — threats that arise from a person or body being too familiar or trusting of another person instead of seeking audit evidence is a familiarity threat to impartiality.

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

4.3 Competence

Competence of the personnel supported by the organizational infrastructure is necessary for the certification body to deliver certification that provides confidence. Competence is the demonstrated ability to apply appropriate knowledge and skills effectively.

4.4 Responsibility

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

4.4.2 The certification body has the responsibility to assess sufficient objective evidence upon which to base a recommendation for certification. Based on audit recommendations 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 Audit evidence shall be verifiable. It is based on samples of the information available, since an audit is conducted during a finite period of time and with finite resources. The appropriate use of sampling is closely related to the confidence that can be placed in the audit conclusions.

4.5 Openness

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

4.5.2 To gain or maintain confidence in certification, a certification body needs to provide appropriate access, or disclosure to, 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, a certification body needs to keep confidential any sensitive, proprietary, and/or vulnerability-related information about an organization's supply chain security management system.

4.7 Resolution of complaints

Parties that rely on certification expect to have complaints investigated and, if these are found to be valid, should have confidence that the complaints will be appropriately addressed and a reasonable effort will be made to resolve the complaints.

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

5 General requirements

5.1 Legal and contractual matters

5.1.1 Legal responsibility

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

5.1.2 Certification agreement

The certification body shall have a legally enforceable agreement for the provision of certification activities to its client organizations. In addition, where there are multiple offices of certification bodies or multiple sites of a certified client, the certification body shall ensure there is a legally enforceable agreement between the certification body granting certification and issuing a certificate, and the certified client, explicitly covering each certified site of the client. The agreement shall clearly define to which standard(s) and/or other normative documents the certification shall take place.

5.1.3 Responsibility for certification decisions

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

5.2 Management of impartiality

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

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

5.2.3 When a relationship gives rise to a threat to impartiality that cannot be eliminated or minimized, such as a wholly owned subsidiary of the certification body requesting certification from its parent, then certification shall not be provided.

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

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

5.2.6 The certification body and any part of the same legal entity shall not offer or provide internal audits to its certified clients. This applies also to that part of government identified as the certification body.

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

NOTE 1 Allowing a minimum period of two years to elapse following the end of the supply chain security management system consultancy and/or associated risk assessments or internal audits is one way of reducing the threat to impartiality to an acceptable level.

NOTE to 5.2.2 and 5.2.4 A relationship that threatens the impartiality of the certification body may be based on ownership, governance, management, personnel, shared resources, finances, contracts, marketing, and payment of a sales commission or other inducement for the referral of new clients, etc.

NOTE to 5.2.6 and 5.2.7 Internal audits in which auditors suggest solutions (to identified nonconformities or opportunities for improvement) are considered an unacceptable threat to impartiality.

5.2.8 The certification body shall not outsource audits to organizations which pose an unacceptable threat to the impartiality of the certification body (see 7.5).

NOTE This clause does not apply to individuals contracted as auditors covered in 7.3.

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

5.2.10 To ensure that there is no conflict of interests, personnel who have provided supply chain security management system consultancy and/or associated risk assessments to the client, including those acting in a managerial capacity, shall not be employed to take part in an audit or certification activities within two years following the end of the consultancy.

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

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

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

NOTE The fact that the organization employing the auditor is known to have provided supply chain security management system consultancy and/or associated risk assessments on the supply chain security management system, within two years following the end of the consultancy, is likely to be considered as a high threat to impartiality.

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 arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations in each of its fields of activities and the geographic areas in which it operates.

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

6 Structural requirements

6.1 Organizational structure and top management

6.1.1 The structure of the certification body shall be such as to give confidence in its certification.

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

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

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

c) supervision of the finances of the body;

d) performance of audits, certification and resolution of complaints;

e) decisions on certification;

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

g) contractual arrangements;

h) providing adequate, qualified resources for certification activities.

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

6.1.4 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 Committee for safeguarding impartiality

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

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

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

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

NOTE Other tasks or duties may be assigned to the committee. However such additional tasks or duties should not compromise its essential role of ensuring impartiality.

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

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

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

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

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

7 Resource requirements

7.1 Competence of management and personnel

7.1.1 The certification body shall ensure all personnel involved in the audit and certification of supply chain operating companies are competent for the roles they carry out.

They shall have processes to ensure that personnel have appropriate knowledge, skills and experience relevant to types of supply chain security management systems and geographic areas in which it operates.

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

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

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

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

7.2 Personnel involved in the certification activities

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

7.2.2 The certification body shall ensure that personnel assigned to perform supply chain security certification audits as well as technical experts, as far as these have contact with confidential information, can be trusted to maintain confidential information obtained during verification work and that they do not create a security breach. See 7.4.

7.2.3 Personnel assigned to perform supply chain security management system audits shall have as a minimum personal attributes, knowledge, skills and education as described in chapter 7.2, 7.3.1, 7.3.2 and 7.4 of ISO 19011:2002 relevant to supply chain security management and risk analysis.

7.2.3.1 The supply chain security management auditor shall have competencies in risk analysis, analysis of critical control points, risk management methodologies, and information confidentiality. This includes but is not limited to:

a) Understanding the requirement of the supply chain security management standard or specification (e.g. ISO/PAS 28000).

b) Understanding supply chain process flow and analysis of critical control points, knowledge of relevant processes and practices within the supply chain.

c) Threat Identification:

   — Understanding threats, such as physical, biological, chemical, cyber, and radiological.

d) Risk Assessment and Analysis:

   — Understanding the principles of risk assessment and analysis.

e) Risk Minimization, Mitigation, and Control:

   — Understanding the principles of risk minimization, mitigation, and management.

— Knowledge of security methodologies and technologies, especially preventative measures and techniques.

f) Incident Planning and Preparedness:

— Knowledge of the role of government and first responders.

— Knowledge of incident communications protocols.

— Knowledge of incident mitigation, response, and recovery.

7.2.3.2 Each supply chain security management system auditor shall also have successfully completed training (see Appendix C or equivalent) and be able to demonstrate competence in the understanding and application of security methodologies and risk analysis and management principles and should be a certified management system auditor.

7.2.3.3 Each supply chain security management system auditor shall undertake appropriate continual training according to their specific qualification requirements. Certification bodies shall annually review a targeted training plan for their auditors on security methodologies, risk analysis and management principles, analysis of critical control points, audit techniques, and in particular on the competence items mentioned under 7.2.3.1 above. This training shall

a) be planned as the result of an analysis of needs on the subjects and competence items given above;

b) be recorded;

c) include audit case studies allowing an auditor's competence to be evaluated;

d) be supported by information such as interpretation of the application of applicable management system standards, FAQs, workshop records, standard correction on case studies and this should be available to the auditor;

e) be evaluated according to training requirements, and certification bodies shall take appropriate action on the basis of the training result; and

f) be performed by qualified trainers.

7.2.3.4 The supply chain security management system auditor shall have a minimum of five years experience relevant to risk analysis and management, or two years when auditing against best industry practices and standards.

7.2.3.5 The supply chain security management system auditor shall perform a minimum of fiverelevant audits per year or carry out a minimum of 10 on-site audit days per year to maintain his/her qualification.

7.2.3.6 The certification body shall be able to demonstrate that every auditor has appropriate training and experience for the particular categories for which they are considered competent. Competence shall be recorded (clause 5.5 c of ISO 19011:2002.)

7.2.4 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.

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

7.2.6 The certification body shall have defined processes for selecting, training, formally authorizing and monitoring auditors and for selecting technical experts used in the certification activity. The initial competence evaluation of an auditor shall include observing an on-site audit undertaken by the person being evaluated.

7.2.7 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. This process shall be based on the guidance provided in ISO 19011 transformed into appropriate documented requirements. (See in particular Clause 7 of ISO 19011:2002 and Annex C.)

7.2.8 Supply chain security auditors shall have knowledge and experience of security applicable to the supply chain and the industrial and business sectors they audit.

7.2.9 Supply chain security management system auditors shall have, or undertake training to acquire and demonstrate the competences described in Annex D.

7.2.10 Competence shall be verified by written examinations. The examination pass mark should be set so that only those candidates that demonstrate a comprehensive understanding of the content of the modules and have achieves the objective of the course will be allowed to pass.

7.2.11 The certification body shall ensure that auditors and, where needed, technical experts, are familiar with certification activities, certification requirements, audit methodology 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.

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

NOTE Assignment of auditors to teams for specific audits is addressed in Clause 9.

7.2.13 The certification body shall identify training needs and shall offer or provide access to specific training to make its auditors, technical experts, and other persons involved in the certification activities, knowledgeable of certification requirements and processes.

7.2.14 The group or individual which takes the decision on granting, maintaining, renewing, extending, reducing, suspending or withdrawing certification shall have knowledge and experience sufficient to evaluate the audit processes and related recommendations of the audit team.

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

7.2.16 The documented monitoring procedures shall include a combination of on-site observation, review of audit reports and feedback from clients or from the market and shall be based on the guidance provided in ISO 19011 transformed into appropriate documented requirements. This monitoring shall be designed in such a way as to minimize the disturbance of the normal processes of certification, especially from the client's viewpoint.

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

7.3 Use of external auditors and external technical experts

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

The certification body shall assure that all individual external auditors and external technical experts undergo security clearance and are bound by all confidentiality agreements of the certification body.

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

7.4 Personnel records

The certification body shall maintain up to date records of relevant qualifications, training, experience, affiliations, professional status and competence of each person involved in the certification activity.

7.4.1 Security clearance

Audit bodies shall establish and document a process for security vetting candidate security auditors.

Accreditation bodies shall also ensure that their auditors meet these requirements.

The process for security vetting auditors shall be documented in a way that can be accessed by organizations applying for security certification or audit and, where applicable other relevant stakeholder organizations.

Auditors shall be security cleared by their respective audit bodies. The security clearance process shall include the following.

7.4.2 Background checks

Certification bodies shall carry out criminal background checks of all personnel; auditors and technical experts who undertake supply chain security management system audits. Where practicable these checks shall be through national security checking agencies or police authorities. Where this is not practicable then the certification body shall check the suitability and integrity through an internal vetting process through a process of records checks and security clearance vetting assessment/interviews, overseen by the organization's top management. The vetting process shall include review of documented submissions by candidate security audit personnel, interviews and reviews of documents such as passport, identity cards, work permits, driving licences and work place references. Those conducting interviews of security auditors shall be appointed and vetted using the process in 7.4.3.

7.4.3 Interviews

The audit body shall establish a hierarchy of interviews which shall be overseen by top management.

Top management shall appoint an accountable manager who has been verified by interview and vetting as trustworthy and having the necessary competence and judgement to vet candidate security auditors and technical experts. The accountable manager shall assess through review of documentation, submitted by candidates, and interviews and ongoing monitoring, the trustworthiness and appropriate behavioural characteristics of candidate security auditors and technical experts.

7.4.4 Work history

Each candidate security auditor shall be able to provide evidence of at least 5 full years continuous work history which shall be verified with current or previous employers. Self employed candidate security auditors shall provide other appropriate documentation that demonstrates the same level of confidence and trustworthiness as employment records.

7.4.5 ID cards

Each security auditor shall be issued with an ID card showing the following:

— photograph;

— first and family name;

— nationality;

— ID card number;

— name and logo of the certification body;

— a mark and feature which prevents alteration and falsification.

When requested confidentiality pledges by security auditors shall be made available to organizations undergoing audit.

7.4.6 Records

The procedure shall include the process that the audit body will implement for security auditors who default. These should include implementing the organization's disciplinary procedure including suspending auditors while investigations are carried out. Records shall be retained for periods that certification bodies deem and justify to be appropriate. National, international and other legal requirements should be taken account of when determining record retention periods.

7.4.7 Auditor accountability

Auditors should be made aware and give written understanding that breaches could subject them to disciplinary actions, civil liability and criminal prosecutions.

7.5 Outsourcing

7.5.1 The certification body shall have a process in which it describes the conditions under which outsourcing (which is contracting with 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 qualifications, confidentiality and conflict of interests, with each body that provides outsourced services.

NOTE 1 This may include outsourcing to other certification bodies. Use of auditors under contract is addressed in 7.3.

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

7.5.2 Decision-making regarding certification shall never be outsourced.

7.5.3 The certification body shall:

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

b) take responsibility for granting, maintaining, renewing, extending, reducing, suspending or withdrawing certification;

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

d) ensure that the body that provides outsourced services uses individuals that 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;

e) obtain the consent of the client to use a given body that provides the outsourced services; and

f) take responsibility for handling complaints and appeals.

7.5.4 The certification body shall have documented procedures for the qualification and monitoring of all bodies that provide outsourced services used for certification activities, and shall maintain records of the qualifications of auditors.

8 Information requirements

8.1 Publicly accessible information

8.1.1 The certification body shall maintain and provide, upon request, information about the activities and geographical areas where it operates.

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

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

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

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

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

8.2 Certification documents

8.2.1 The certification body shall provide by any means it chooses (see Note 1 to 8.1.4) certification documents to the certified client.

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

8.2.3 The certification document(s) shall identify:

a) the name and identifiable physical location(s) of each site of the client organization whose supply chain security management system is certified;

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

c) the expiry date consistent with the re-certification cycle;

d) a unique identification code;

e) the standard(s) and/or other normative document including issue and/or revision used for assessment of the certified client;

f) the scope of certification applicable to activities undertaken within the client's supply chain security management system including service, process, etc. as applicable at each site;

g) the name and/or certification mark of the certification body;

NOTE If the certification body is entitled to do so, other marks (e.g. accreditation symbol) may be used; however, the certification body as the issuing authority for the certificate should ensure that the meaning of the mark(s) is not misleading or ambiguous.

h) any other information required by the standard used for certification.

8.3 Directory of certified clients

The certification body shall maintain and make available to the public, by any means it chooses, a directory of valid certificates that as a minimum shall show the name, relevant normative document, scope of the activities and organizational elements, geographical location (city/town and country) for each certified client.

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

8.4 Reference to certification and use of marks

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

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

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

8.4.3 The certification body shall require that the client organization:

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

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

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

f) does not allow reference to its supply chain security management system certification to be used to imply that the certification body certifies any supply chain or any element of a supply chain;

g) does not imply that the certification applies to activities 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.

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

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

8.5 Confidentiality

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

8.5.2 The certification body shall inform the client, in advance, of the information (as defined in 4.5.1 and 8.3) it intends to place in the public domain. All other information, except for information that is made publicly available by the client, shall be considered confidential.

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

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

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

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

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

8.6 Information exchange between a certification body and its clients

8.6.1 Information on the certification activity and requirements

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

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

b) the normative requirements for certification;

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

d) the certification body’s requirements for the prospective client:

   1) to comply with certification requirements;

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

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

f) information on procedures for handling complaints and appeals.

8.6.2 Notice of changes by a certification body

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

NOTE Contractual arrangements with certified clients may be necessary to ensure implementation of this clause.

8.6.3 Notice of changes by a client

The certification body shall have legally enforceable arrangements to ensure that the certified client informs the certification body, without delay, of matters that may affect the capability of the supply chain security management system to continue to fulfill the requirements of the standard used for certification, e.g. changes relating to:

a) 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 supply chain security management system;

e) major changes to the supply chain security management system and processes.

8.6.4 Information about the supply chain security management system

The certification body shall have procedures in place which ensure a secure exchange of information regarding the functioning of the clients supply chain security management system between the certification body, its client and other parties which is permitted access to the information. The certification body shall ensure that clients and these other parties are timely informed about these procedures.

9 Process requirements

9.1 General requirements applicable to any audit

9.1.1 The audit programme shall include an audit comprising at least a 2 stages initial audit, surveillance audits, and a recertification audit. The determination of audit programme and any subsequent adjustments shall consider the size of the client, the scope and complexity of its supply chain security management system and processes as well as demonstrated level of supply chain security management system effectiveness and the results of any previous audits.

9.1.2 The certification body shall ensure that an audit plan, based on the guidance provided in ISO 19011, transformed into appropriate documented requirements for preparing the audit plan. It is established for each audit to provide the basis for agreement regarding the conduct and scheduling of the audit activities.

9.1.3 The certification body shall have a process for selecting and appointing the audit team, including the audit team leader, taking into account the competence needed to achieve the objectives of the audit. This process shall be based on the guidance provided in ISO 19011, transformed into appropriate documented requirements.

9.1.4 The certification body shall have formal rules and/or contractual conditions to ensure that each team member acts in an impartial manner. Each team member shall inform the certification body, prior to accepting assignment of the audit, about any known existing, former or envisaged link to the organization to be audited (see also 5.2.9, 5.2.12 and 7.4).

9.1.5 The certification body shall determine, in accordance with documented procedures, the auditor time needed to accomplish a complete and effective audit of the client's supply chain security management system at the locations included in the scope of certification.

9.1.6 Security threats are unique to each operational site; therefore all operational sites included in an organization's scope of certification/registration shall be subject to audit. The organization shall have carried out a threat and risk assessment for each site and shall implement operational controls accordingly. Similarly, security threats applicable to non operational sites, such as those providing support administrative services, are also unique but by the nature of the activities undertaken may present a lower risk to supply chain

security. All operational sites shall be subject to certification/registration body audits and the risks presented by other non operational sites shall be evaluated and audited commensurate to those risks.

The auditor time determined by the certification body for each site/location, and the justification for the determination, shall be based on the requirements in Annexes A and B and be recorded. In determining the auditor time, the certification body should consider, among other things, the following aspects:

a) the requirements of the relevant supply chain security management system standard;

b) complexity;

c) size;

d) risks;

e) technological and regulatory context; and

f) number of sites and multiple site considerations. Requirements for organizations that operate multiple sites are described in Annex B.

The auditor mandays shall be based on the manday tables shown in Annex A. Although Annex A is informative the mandays for the audit of a supply chain operating company are unlikely to be less than those shown in Annex A.

9.1.7 Sampling is not appropriate for organizations that operate multiple operational sites, even where the activities are substantially the same. Each site included in the scope of certification shall be audited, however, there may be a case for reducing the duration of the audit for some sites where the supply chain security management system and the activities at the various locations are the same or sampling some non operational sites where the activities carried out are mainly administrative and do not impact significantly on supply chain security. In these cases the certification body shall undertake a risk assessment and develop a risk based audit programme for each site. This process shall ensure that a proper audit of the supply chain security management system operated by the organization is audited by the certification body. This requirement is further described in Annex B.

9.1.8 In the event of the preparation of the audit plan being assigned to someone other than the audit team leader, the audit team leader shall review and approve the plan.

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

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

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

c) determine that the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the supply chain security management system of the client organization;

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

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

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

9.1.12 The certification body shall have a process for conducting on-site audits based on the guidance provided in ISO 19011, transformed into an appropriate documented procedure.

NOTE 1 In addition to visiting physical location(s) (e.g. factory), 'on-site' can include remote access to electronic site(s) that contains information that is relevant to the assessment of the supply chain security management system.

NOTE 2 The term auditee as used in ISO 19011 means the organization being audited.

9.2 Initial audit and certification

9.2.1 Application

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

a) the desired scope of the certification;

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

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

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

e) information concerning the use of consultancy relating to the supply chain security management system.

9.2.2 Application review

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

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

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

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

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

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

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

9.2.2.2 Based on this review, the certification body shall determine the competences it needs to include in its audit team and for the certification decision (see 7.2.7).

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

9.2.2.4 After having conducted the application review, the certification body shall notify the applicant that it is accepting or not accepting the application. The reasons for non-acceptance shall be conveyed to the applicant.

9.2.2.5 Before commencing the audit, an agreement (see 5.1.2) shall be established between the certification body and the applicant organization which:

a) defines the scope of work to be undertaken, including the intended scope of certification and site details;

b) requires the applicant organization to supply any information needed for its intended certification;

c) requires the applicant organization to comply with the requirements for certification.

9.2.2.6 The certification body shall, in response to an application for extension to scope of a certification already granted, undertake a feasibility review and audit activities necessary to determine whether or not the extension may be granted.

9.2.2.7 The audit team shall be appointed (see 9.1.3) and composed of auditors (and technical experts as necessary) who, between them, have the totality of the competences identified by the certification body as set out in 9.2.2.2) for the certification of the applicant organization. The selection of the team shall be performed with reference to the designations of competence of auditors and technical experts made under Clause 7.2.5, and may include use of both internal and external human resources.

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

9.2.2.9 The audit team needs a background which ensures that the members understand the requirements relating to the system they are auditing. Each audit team shall have a general understanding and background in each technological and industrial sector in which it operates. It shall be able to determine whether or not a particular Supply Chain Security Management System Standard adequately complies with the requirements of the standard.

9.2.2.10 The above requires that the audit team, deployed in each case by a certification body to conduct an audit of an organization's Supply Chain Security Management System Standard, needs to know what elements, general to the processes and procedures, are essential to the supply chain in question. The audit team shall have the necessary competence, including sector or regulatory credentials, to determine whether the system covers these essential elements in a manner that gives adequate confidence that the system can be assured to meet specified requirements.

9.2.2.11 In certain instances, particularly where there are critical requirements and special procedures, the background knowledge of the audit team may be supplemented by briefing, specific training or experts in attendance. The certification body may attach non-auditor experts to their audit teams. If a certification body does use technical experts, its management control systems shall provide for it and for keeping competence up to date. The documentation shall include details of how technical experts are selected and how their competence is assured. The certification body may rely on outside help, for example, from industry or professional institutions.

The certification body shall ensure that personnel provided to perform this clause are bound by the same requirements as auditors for confidentiality and impartiality.

9.2.3 Initial certification audit

The initial certification audit of a supply chain security management system shall be conducted in two stages - stage 1 and stage 2.

9.2.3.1 Stage 1 audit

9.2.3.1.1 Stage 1 audits shall have an audit plan that addresses the points defined in 9.1.2 and 9.2.3.1.2.

9.2.3.1.2 Normally the audit team shall perform the stage 1 audit of a client organization's supply chain security management system on-site. In exceptional cases stage 1 could be carried out without a visit. The decision not to visit the site shall be justified and documented and the client shall be informed it creates a risk

for the stage 2 audit. Such justification should be based on the organizations size, location, risk considerations, previous knowledge, etc.

9.2.3.1.3 The stage 1 audit shall be performed to:

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

b) review the client organization'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 supply chain security management system;

c) collect and review necessary information regarding the scope of the supply chain security management system, information about the risk assessment performed, processes and location(s) of the client organization, and related statutory, regulatory aspects and compliance, e.g., legal aspects of the applicant organization's operation, identified risks, etc.;

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

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

f) evaluate if the internal audits and management review are being planned and performed and that the level of implementation of the supply chain security management system substantiates that the client organization is ready for the stage 2 audit.

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

9.2.3.1.5 Any part of the supply chain security management system that is audited during the stage 1 audit and determined to be fully implemented, effective, and in conformity with requirements, may not need to be re-audited during the stage 2 audit, however the certification body has to ensure that the already audited parts of the supply chain security management system continue to conform to the certification requirements. In this case the stage 2 audit report shall include these findings and clearly state that conformity has been established during the stage 1 audit.

9.2.3.1.6 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 the stage 1 audit. The certification body may also need to revise its arrangements for stage 2.

9.2.3.2 Stage 2 audit

9.2.3.2.1 Stage 2 audits shall have an audit plan (see 9.1.2). The plan shall follow the guidance in ISO 19011 transformed into appropriate documented requirements and take into account the information obtained during the stage 1 audit.

9.2.3.2.2 The stage 2 audit shall take place at the site(s) of the client organization. The purpose of the stage 2 audit is to evaluate the implementation and effectiveness of the client's supply chain security management system.

9.2.3.2.3 The audit team shall conduct the stage 2 audit to gather audit evidence that the supply chain security management system conforms to the standard and other certification requirements.

9.2.3.2.4 The audit team shall audit a sufficient number of examples of the activities of the client organization in relation to the supply chain security management system and activities to get a sound appraisal of the implementation, including effectiveness, of the supply chain security management system.

9.2.3.2.5 As part of the audit, the audit team shall interview a sufficient number of the staff, including top management and operational personnel of the audited facility, to provide assurance that the system is implemented and understood throughout the client organization.

9.2.3.2.6 The audit team shall analyze all information and audit evidence gathered during the stage 1 and stage 2 audits to determine the extent of fulfillment with all certification requirements and decide on any nonconformity. The audit team may propose opportunities for improvement but shall not recommend specific solutions.

9.2.3.2.7 The stage 2 audit shall cover an examination of the organization's supply chain security management system which address at least the following:

a) information and evidence about conformity to all requirements of the applicable normative document;

b) performance monitoring, measuring, reporting and reviewing against key performance objectives and targets;

c) the organization's supply chain security management system and performance as regards legal and regulatory compliance;

d) operational control;

e) internal auditing and management review;

f) management responsibility for the client organization's policies;

g) links between the normative requirements, policy, performance objectives and targets, any applicable legal requirements, responsibilities, personnel competence, operations, procedures, performance data, and internal audit results.

9.2.3.2.8 Action that shall be undertaken after the completion of a stage 2 audit shall include at least the following:

a) a record of any identified and agreed nonconformities shall be left with the client prior to departure from the audit site;

b) establishing the audit report specified in 9.2.4.

9.2.3.2.9 Nonconformity shall be defined as the absence of, or the failure to implement and maintain, one or more quality management system requirements, or a situation which would, on the basis of available objective evidence, raise significant doubt as to the quality of what the organization is supplying.

The certification/registration body is free to define different grades of deficiency and areas for improvement (e.g. Major and Minor Nonconformities, Observations, etc.).

9.2.4 Initial certification audit reports

9.2.4.1 The certification body shall have documented reporting procedures.

9.2.4.2 The stage 1 audit report shall include comments on the adequacy of the supply chain security management system documentation, the organization's analysis of key performance or significant aspects and whether the level of implementation of the supply chain security management system indicates that it is ready for the stage 2 audit. The stage 1 audit report shall report on the requirements in 9.2.3.1.3.

9.2.4.3 The stage 2 audit report shall be based on the guidance provided in ISO 19011 transformed into appropriate documented requirements.

9.2.4.4 The auditor's internal audit report shall at least include or refer to the following:

a) identification of the audit client;

b) identification of the auditee representatives;

c) identification of the certification body;

d) identification of audit team leader and members;

e) the audit objectives;

f) the audit scope, particularly identification of the organizational and functional units or processes audited, the time period covered and the elements of the supply chain assessed;

g) the audit criteria;

h) the reference to the supply chain security management standards and/or other normative reference documents used;

i) the dates and sites where the on-site audit activities were conducted and the date of the previous audit;

j) the audit findings:

1) summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the supply chain security management system;

2) overview and summary of the most constructive/beneficial information, positive as well as negative, regarding the implementation and effectiveness of the risk assessment methodology;

3) nonconformities raised during the audit against specific standard requirements;

4) report on the clearing of each nonconformity revealed previously;

k) the audit conclusions:

1) degree of reliance that can be placed in the supply chain security management system and risk assessment methodology;

2) audit team recommendations regarding certification status.

9.2.4.5 As a minimum these documented procedures shall ensure, after a stage 2 audit, that a written client audit report is provided within a mutually agreed period of time to the audited organization, including audit findings and conclusions, positive and negative, on fulfilment, including effectiveness, of the supply chain security management system (in particular, referencing the effectiveness of the internal audit process and achievement of policy commitments) with all requirements of the standard, including identifying any nonconformities.

9.2.4.6 Ownership of the audit report shall be maintained by the certification body. Where the contents of reports include security sensitive data then custody of the report may be delegated to the organization, but ownership and the right to amend reports remains with the certification body.

9.2.5 Post-audit activities

9.2.5.1 The audited organization shall be requested to describe the specific correction and corrective actions taken, or planned to be taken, to eliminate detected nonconformities and their causes, within a defined time, to remedy any identified nonconformities.

9.2.5.2 The audited organization shall be informed if an additional full audit, an additional limited audit, or documented evidence (to be confirmed during future surveillance audits), will be needed to ensure effective

correction and corrective actions. This decision will be based on the types and number of nonconformities identified.

9.2.5.3 Correction and corrective actions by the audited organization shall be reviewed by the certification body to determine if the actions are sufficient and, if already implemented, effective.

9.2.6 Initial certification decision granting or extending certification

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

a) the reports indicated in 9.2.4;

b) comments on the nonconformities, and the correction and corrective actions taken by the audited organization;

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

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

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

9.2.6.3 The certification body shall ensure that the person(s) or committees that participate in the certification decisions are different from those who carried out the audits.

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

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

b) it has reviewed and accepted the performance of satisfactory correction and corrective action, including actions to eliminate the cause to prevent recurrence, for all nonconformities that denote either:

   1) absence of, or failure to, implement and maintain the fulfilment of one or more supply chain security management system requirements; or

   2) a situation that, on the basis of available objective evidence, would raise significant doubt as to the capability of the client organization to meet requirements consistently and the effectiveness of the supply chain security management system;

c) for any other nonconformities, it has accepted the organization's planned activities of correction and corrective action including actions to prevent recurrence.

9.3 Surveillance activities

9.3.1 General

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

9.3.1.2 Surveillance activities shall include on-site audits assessing the certified client's supply chain security management system's fulfillment of specified requirements with respect to the standard(s) and other normative documents to which the certification is granted. Other surveillance activities may include:

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

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

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

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

9.3.1.3 The certification body shall have an established programme for carrying out periodic surveillance audits at sufficiently close intervals to confirm that the certified supply chain security management system continues to fulfill all certification requirements and to be effective.

9.3.1.4 The date of the first surveillance audit, following initial certification, shall be programmed from the end of stage 2 of the initial audit (e.g. from the date of the closing meeting).

9.3.2 Surveillance audit

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

a) internal audits, security assessment and planning, and management review;

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

c) treatment of complaints;

d) effectiveness of the supply chain security management system with regard to achieving the certified client's objectives;

e) progress of planned activities aimed at continual improvement;

f) continuing operational control;

g) review of any changes; and

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

9.3.2.2 Surveillance audits shall be conducted at least once a year

9.3.2.3 Surveillance audits shall have a audit plan (see 9.1.2).

9.3.2.4 The duration of a surveillance audit shall take account of the guidance in Annex A and be determined by the certification body with due regard to:

a) the risk category of the processes and elements of the supply chain;

b) the number of supply chain elements, sites, processes and products;

c) the number of employees related to supply chain security;

d) the size of the random sampling;

e) the number of nonconformities observed at previous audits;

f) changes in the organization, products or processes.

9.3.3 Surveillance audit report

9.3.3.1 For surveillance audits, the report from the audit team shall include:

a) the supply chain security management system standard requirements that were audited;

b) comments on the fulfillment of certification requirements, including effectiveness;

c) verification of the effective implementation of corrective action for every nonconformity from the audit; and

d) any new nonconformities.

This report shall be based on the guidance provided in ISO 19011 transformed into appropriate documented requirements.

9.3.3.2 This report shall be provided to the certified client and to the certification body.

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

NOTE It is recommended that time limits be based on the severity of the nonconformity and its impact.

9.3.3.4 The audited organization shall be informed if an additional full audit, an additional limited audit, or documented evidence (to be confirmed during future surveillance audits), will be needed to ensure effective correction and corrective actions. This decision will be based on the types and number of nonconformities identified.

9.3.4 Maintaining certification

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

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

b) the criteria to deal with nonconformities and any subsequent corrective actions are known by the team leader;

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

9.4 Recertification

9.4.1 Recertification cycle

The time interval between the initial certification audit and re-certification audit or between two re-certification audits shall not exceed 3 years.

9.4.2 Recertification audit plan

9.4.2.1 A recertification audit shall be planned and conducted to evaluate the continued fulfillment of all of the requirements of the relevant normative document. The purpose of the recertification audit is to confirm the continued conformity and effectiveness of the supply chain security management system as a whole, and its continued relevance and applicability for the scope of certification.

9.4.2.2 The recertification audit shall consider the performance of the supply chain security management system over the period of certification, and include the review of previous surveillance audit reports (9.3.3).

9.4.2.3 Recertification audit activities do not need to have a stage 1 audit in situations where there have been no significant changes to the supply chain security management system, the organization, or the context in which the supply chain security management system is operating (e.g. changes to legislation).

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

9.4.2.5 The results of recent surveillance audits and the certified client's internal audit(s) should be taken into account. The audit plan shall be based on the guidance in ISO 19011 transformed in appropriate documented requirements.

9.4.2.6 The duration of recertification audits shall be based on the guidance in Annex A.

9.4.3 Recertification audit

The recertification audit shall include an on-site audit (which may replace or extend a regular surveillance audit). This recertification audit shall address the following supply chain security management system requirements:

a) the effective interaction between the processes of the supply chain security management system;

b) the effectiveness of the supply chain security management system in its entirety in the light of internal and external changes;

c) demonstrated commitment to maintain the effectiveness and improvement of the supply chain security management system in order to enhance overall performance;

d) that the operation of the certified supply chain security management system contributes to the achievement of the organization's policy and objectives.

9.4.4 Recertification audit report

9.4.4.1 For recertification audits, the report from the audit team to the certified client and to the certification body shall comment on the following:

a) the supply chain security management system reviewed including risk analysis;

b) the fulfillment of certification requirements;

c) the review and verification of the continued effective implementation of corrective action for every nonconformity from the previous audit; and

d) the effectiveness of the audited organization's supply chain security management system.

This report shall be based on the guidance provided in ISO 19011 transformed into appropriate documented requirements.

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

NOTE It is recommended that the time limits should be based on the severity of the nonconformity and its impact, and not be so long as to have the credibility of the certification called into question.

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

9.4.5 Recertification decision

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

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

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

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

b) it has reviewed and accepted the performance of satisfactory correction and corrective action, including actions to eliminate the cause to prevent recurrence, for all nonconformities that denote either:

   1) failure to maintain the fulfilment of one or more supply chain security management system requirements; or

   2) a situation that, on the basis of available objective evidence, would raise significant doubt as to the capability of the client organization to meet requirements consistently and the effectiveness of the supply chain security management system;

c) for any other nonconformities, it has accepted the organization's planned activities of correction and corrective action including actions to prevent recurrence.

9.5 Special audits

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

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

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

9.6 Suspending, withdrawing or reducing scope of certification

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

9.6.2 The certification body shall suspend certification in cases when, but not limited to:

a) the client's certified supply chain security management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the supply chain security management system;

b) the certified client does not allow surveillance or recertification audits to be conducted at the required frequencies; or

c) the certified client has voluntarily requested a suspension.

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

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

NOTE In most cases the suspension should not exceed six months.

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

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

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

9.7 Appeals

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

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

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

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

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

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

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

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

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

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

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

9.8 Complaints

Clients and users of certification (see 4.1.2 and 4.7) can expect to have complaints investigated, and if determined to be valid, have confidence that the complaints will be appropriately addressed and that a reasonable effort will be made to resolve the complaint.

NOTE The effective resolution of complaints is an important means of protection for the certification body, its clients, the bodies authorizing certification bodies and other users of certification against errors, omissions or unreasonable behavior. Confidence in certification activities is safeguarded when complaints are processed appropriately.

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

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

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

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

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

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

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

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

NOTE ISO 10002 provides guidance for handling complaints.

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

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

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

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

9.8.10 The certification body shall determine together with the client and the complainant whether, and if so to what extent, the subject of the complaint and its resolution shall be made public. Any decision to keep the complaint confidential is subject to appeal by any party to the complaint and shall be justified.

9.9 Records on applicants and clients

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

9.9.2 Records on certified clients shall include:

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

b) justification of the methodology used for any reduction of audit durations;

c) justification for auditor time determination (see 9.1.5);

d) verification of correction and corrective actions;

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

f) committee deliberations and decisions, if applicable;

g) documentation of the certification decisions;

h) certification documents including the scope of certification with respect to product (including services) or process as applicable; and

i) related records necessary to establish the credibility of the certification, such as evidence of auditor and technical expert qualifications and competency.

9.9.3 The certification body shall keep the records on 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 (see 10.2.3).

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

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

10 Management system requirements for certification bodies

The certification body shall establish and maintain a management system that is capable of supporting and demonstrating the consistent achievement of the requirements of this International Standard. In establishing its management system the certification body shall implement a management system in accordance with the requirements contained in 10.1 or 10.2.

10.1 Option 1 — Management system requirements in accordance with ISO 9001

The certification body shall establish and maintain a management system, in accordance with the requirements of ISO 9001 that is capable of supporting and demonstrating the consistent achievement of the requirements of this International Standard, amplified by 10.1.1 to 10.1.4.

10.1.1 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.

10.1.2 Customer focus

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

10.1.3 Management review

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

10.1.4 Design and development

For application of the requirements of ISO 9001, when developing a new management system certification scheme, or adapting an existing one to special circumstances, the certification body shall ensure that the guidance given in ISO 19011, and which is appropriate to third-party situations, is included as a design input.

10.2 Option 2 — General management system requirements

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

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

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

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.

10.2.1 Management system manual

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

10.2.2 Control of documents

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

a) to approve documents for adequacy prior to issue;

b) to review and update as necessary and re-approve documents;

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

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

e) to ensure that documents remain legible and readily identifiable;

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

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

10.2.3 Maintenance and destruction of documents of a sensitive nature

The certification body shall establish and implement procedures to ensure that clients' documents and records of a security sensitive nature and the information and data derived from audits such as auditors' notes are kept secure at all times and are archived and subsequently destroyed with due regard to there security classification.

Documents, data and records of a security sensitive nature shall only be made available to certification body's personnel and others external to the certification body on a need to know basis by those who are covered by the appropriate level of security clearance.

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 International Standard.

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

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

10.2.5 Management review

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

10.2.5.1 Review inputs

The input to management review shall include information related to:

a) results of audits;

b) feedback from clients and interested parties related to the fulfillment of this International Standard;

c) status of preventive and corrective actions;

d) follow-up actions from previous management reviews;

e) fulfilment of objectives;

f) changes that could affect the management system;

g) appeals and complaints.

10.2.5.2 Review outputs

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

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

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

c) resource needs.

10.2.6 Internal audits

10.2.6.1 The certification body shall establish procedures for internal audits to verify that it fulfills the requirements of this International Standard and that 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 a year. The frequency of internal audits may be reduced if the certification body can demonstrate that its management system continues to be effectively implemented according to this International Standard and has proven stability.

10.2.6.4 The certification body shall ensure that:

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

b) auditors shall 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 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 results of actions taken;

g) reviewing effectiveness of corrective actions.

10.2.8 Preventive actions

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

a) identifying potential nonconformities and their causes;

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

c) determining and implementing the action needed;

d) recording results of actions taken;

e) reviewing effectiveness of the preventive actions taken.

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

Annex A
(informative)

Guide for process to determine auditor time

Table A.1 specifies the number of audit days of the initial audit (stage 1 and stage 2) depending on the number of employees and complexity and/or risk of the organization (see note 8).

Table A.1 — Number of audit days for initial audit

Continuum number of effective employees. See note 2 below	Average Mandays (medium complexity and /or risk)	Minimum mandays (low complexity and/or risk)	Typical mandays high complexity and/or risk)	Reduction if organization is certified to another management system (MS) standard or security code which is integrated with the security MS
1 (see 9 below)	1	1	1	0
10	3	3	3	0
30	6	4	8	<20%
100	8	5	11	<20%
500	12	9	15	<20%
2000	15	10	20	<20%

Notes.

If the audit team requires the help of translators with understanding written material then the time above should be increased by 10% and a further 10% if verbal translators are required.

Typically the stage 1 part of the audit will be about 1/3 of the mandays above and the stage 2 the remainder.

Guidance for calculating mandays

The starting point for mandays will be based on the number of effective employees in Table A.1.

1 All attributes of the organization's facility, site, systems, processes, and products/services should be considered and a fair adjustment can be made based on the justifiable factors in Table A.1. Additive factors may be off-set by subtractive factors. In all cases where adjustments are made to the time provided in the Auditor Time table, sufficient evidence and records shall be maintained to justify the variation.

A site plan should be obtained especially for large site and organizations to help with evaluating mandays for the audit so that all features of the site and facilities can be considered. Consideration should be given to site vulnerabilities, neighbouring assets and the closeness of roads, rivers and other access points etc.

2 "Effective employees" are those individuals described in the organization's management system and covered by the scope of the certification including non-permanent (seasonal, temporary, and sub-contracted) staff, whose work has the potential to affect security in the organization being audited. A certification body should agree with the organization to be audited the timing of the audit which will best demonstrate the full scope of the organization. The consideration could include season, month, day/date and shift as appropriate.

Part-time employees should be treated as full-time-equivalent employees. This determination will depend upon the number of hours worked as compared with a full-time employee, see 7 below for calculation of the impact of shifts. When calculating effective employees due consideration should be given to those persons whose work impact on supply chain security. E.g. Those employed in the finance department may not impact as much as those employed directly in manual processes.