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.