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.

