PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 28003

First edition
2006-10-01

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 sureté pour la chaîne d'approvisionnement

Reference number
ISO/PAS 28003:2006(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standard s is normally carried out through ISO technical committees. Each member body interested in a subject for which 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.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an ISO/PAS, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an ISO/PAS or be withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

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

ISO/PAS 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 Publicly Available Specification 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 Publicly Available Specification. This wording should not be an obstacle to the use of this Publicly Available Specification by bodies with other designations that undertake activities covered by the scope of this Publicly Available Specification. Indeed, this Publicly Available Specification 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 Publicly Available Specification 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 Publicly Available Specification 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 Publicly Available Specification aims at being the basis for recognition of the competence of certification bodies in their provision of supply chain security management system certification. This Publicly Available Specification 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 Publicly Available Specification 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 Publicly Available Specification should 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/PAS 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/PAS 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 Publicly Available Specification 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 Publicly Available Specification 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/PAS 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 Publicly Available Specification has been developed to assist in the certification of supply chain security management systems that fulfil the requirements of ISO/PAS 28000, *Specification for security management systems for the supply chain*. The contents of this Publicly Available Specification may also be used to support certification of supply chain security management systems that are based on other sets of specified supply chain security management system requirements.

This Publicly Available Specification

- provides harmonized guidance for the accreditation of certification bodies applying for ISO/PAS 28000 (or other sets of 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 ISO/PAS 28000 requirements (or other sets of specified supply chain security management system requirements);
- provides 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 Publicly Available Specification 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/PAS 28000:2005, *Specification for security management systems for the supply chain*