PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 28004

First edition
2006-09-01

Security management systems for the supply chain — Guidelines for the implementation of ISO/PAS 28000

Systèmes de management de la sûreté pour la chaîne d'approvisionnement — Lignes directrices pour la mise en application de l'ISO/PAS 28000

Reference number
ISO/PAS 28004:2006(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

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 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.

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 International Standard, 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 International Standard 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 28004 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

Introduction

ISO/PAS 28000:2005, *Specification for security management systems for the supply chain* and this Publicly Available Specification have been developed in response to the need for a recognizable supply chain management system standard against which their security management systems can be assessed and certified and for guidance on the implementation of such a standard.

ISO/PAS 28000 is compatible with the ISO 9001:2000 (Quality) and ISO 14001:2004 (Environmental) management systems standards. They facilitate the integration of quality, environmental and supply chain management systems by organizations, should they wish to do so.

This Publicly Available Specification includes a box at the beginning of each clause/subclause, which gives the complete requirements from ISO/PAS 28000; this is followed by relevant guidance. The clause numbering of this Publicly Available Specification is aligned with that of ISO/PAS 28000.

This Publicly Available Specification will be reviewed or amended when considered appropriate. Reviews will be conducted when ISO/PAS 28000 is revised.

This Publicly Available Specification does not purport to include all necessary provisions of a contract between supply chain operators, suppliers and stakeholders. Users are responsible for its correct application.

Compliance with this Publicly Available Specification does not of itself confer immunity from legal obligations.

Security management systems for the supply chain — Guidelines for the implementation of ISO/PAS 28000

1 Scope

This Publicly Available Specification provides generic advice on the application of ISO/PAS 28000:2005, *Specification for security management systems for the supply chain*.

It explains the underlying principles of ISO/PAS 28000 and describes the intent, typical inputs, processes and typical outputs, for each requirement of ISO/PAS 28000. This is to aid the understanding and implementation of ISO/PAS 28000.

This Publicly Available Specification does not create additional requirements to those specified in ISO/PAS 28000, nor does it prescribe mandatory approaches to the implementation of ISO/PAS 28000.

ISO/PAS 28000

1 Scope

This Publicly Available Specification specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. Security management is linked to many other aspects of business management. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

This Publicly Available Specification is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

a) establish, implement, maintain and improve a security management system;

b) assure compliance with stated security management policy;

c) demonstrate such compliance to others;

d) seek certification/registration of its security management system by an Accredited third party Certification Body; or

e) make a self-determination and self-declaration of compliance with this Publicly Available Specification.

There are legislative and regulatory codes that address some of the requirements in this Publicly Available Specification. It is not the intention of this Publicly Available Specification to require duplicative demonstration of compliance.

Organizations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.

2 Normative references

No normative references are cited. This clause is included in order to retain clause numbering similar to ISO/PAS 28000.

3 Terms and definitions

ISO/PAS 28000

3 Terms and definitions

3.1
facility
plant, machinery, property, buildings, vehicles, ships, port facilities and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service

NOTE This definition includes any software code that is critical to the delivery of security and the application of security management.

3.2
security
resistance to intentional, unauthorized act(s) designed to cause harm or damage to or by, the supply chain

3.3
security management
systematic and coordinated activities and practices through which an organization optimally manages its risks and the associated potential threats and impacts there from

3.4
security management objective
specific outcome or achievement required of security in order to meet the security management policy

NOTE It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.

3.5
security management policy
overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements

3.6
security management programmes
the means by which a security management objective is achieved

3.7
security management target
specific level of performance required to achieve a security management objective

3.8
stakeholder
person or entity having a vested interest in the organization's performance, success or the impact of its activities

NOTE Examples include customers, shareholders, financiers, insurers, regulators, statutory bodies, employees, contractors, suppliers, labour organizations or society.