PUBLICLY
AVAILABLE
SPECIFICATION

ISO/PAS 28004-3

First edition
2012-07-15

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

Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

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

Partie 3: Lignes directrices spécifiques supplémentaires concernant la mise en oeuvre de l'ISO 28000 pour l'utilisation dans les petites et moyennes affaires (autres que les ports marins)

Reference number
ISO/PAS 28004-3:2012(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 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 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 28004-3 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

ISO/PAS 28004 consists of the following parts, under the general title *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000:*

- *Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations*

- *Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)*

- *Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective*

Introduction

"**ISO 28000:2007, *Specification for security management systems for the supply chain***", and the guidance contained in ISO 28004, have been developed in response to the need for a recognizable supply chain management system evaluation criteria (validation process) against which their security management systems can be assessed and certified for determining conformance with ISO 28000 and ISO 28004. The guidance currently contained in ISO 28004 is designed to assist organizations adopting ISO 28000. Because the types of organizations that can use ISO 28000 are vast, the guidance provided in ISO 28004 is general in nature. As a result, some smaller organizations have had difficulty in defining the scope of measures needed to address each of the requirements established in ISO 28000. Therefore, the purpose of this part of ISO/PAS 28004 is to provide guidance and amplifying information that can be used by Medium and Small Businesses (other than marine ports) to assist them in defining the scope of validation and verification measures needed to comply with the security provisions specified in ISO 28000 and ISO 28004.

ISO 28000 requires that stakeholder organizations evaluate the capabilities of their security protection management plans and procedures through periodic reviews, testing, post-incident reports, and training exercises to measure the effectiveness of their installed security protection systems and methods. It is critical to the overall continued end-to-end safety of the supply chain that stakeholder organizations ensure the transportation industry that they have sufficient safeguards in place to protect the integrity of the supply chain while those goods are under their direct control. The failure by one of the stakeholder organizations to protect the supply chain from any one of the global threats and operational risks can severely impact the integrity of the system and erode the confidence of those who depend on the secure transportation of their valuable goods.

Medium and small businesses stakeholder organizations are an integral part of the supply transportation system and will be required to conduct these performance capabilities reviews and verify to the transportation industry that they are in conformance with relevant legislation and regulations, industry best practices and conformance with its own security policy and objectives based on the identified threats and risks to their operations. The information contained in this part of ISO/PAS 28004 provides guidance and criteria for evaluating the quality of medium and small businesses (other than marine ports) security management plans developed in accordance with ISO 28000 to protect the integrity of the supply chain. The amplifying information is designed to enhance, but not alter, the general guidance currently specified in ISO 28004. No alterations to ISO 28004, other than the addition of supplements, are made.

Disclaimer

This part of ISO/PAS 28004 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. Conformance with this part of ISO/PAS 28004 does not of itself confer immunity from legal obligations.

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

Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

1 Scope

This part of ISO/PAS 28004 has been developed to supplement ISO 28004-1 by providing additional guidance to medium and small businesses (other than marine ports) that wish to adopt ISO 28000. The additional guidance in this part of ISO/PAS 28004, while amplifying the general guidance provided in the main body of ISO 28004-1, does not conflict with the general guidance, nor does it amend ISO 28000.

1.1 Additional guidance

ISO 28000 is designed to be adopted by any size organization interested in better securing their supply chain or services they provide to supply chain operators. The main body of ISO 28004 is designed to provide guidance to organizations of any size that wish to adopt ISO 28000. Because ISO 28004 is designed to provide guidance to a wide size range of organizations it may appear more complex than is needed by a smaller sized organization. The purpose of this part of ISO/PAS 28004 is to simplify the guidance for use by smaller sized organization. Entities using this part of ISO/PAS 28004 for guidance should refer to the main body of ISO 28004 when more information on specific issues is needed than is provided in this part of ISO/PAS 28004. The guidance provided in this part of ISO/PAS 28004 does not amend ISO 28000 or the main body of ISO 28004. Where specific methodologies are discussed in this part of ISO/PAS 28004 they are provided for illustrative purposes (to explain what needs to be accomplished) and other methodologies could be substituted.

Organizations adopting ISO 28000 will need to;

- Specify what their objectives are in regard to providing supply chain security,
- Assess the current state of supply chain security,
- Develop plans that will include existing supply chain processes and procedures, and any additional processes/procedures or systems that have been identified as necessary to meet the stated supply chain security objectives,
- Train personnel as to their duties and responsibilities as defined in the supply chain security plan,
- Install/maintain any systems or equipment specified in the supply chain security plan,
- Begin execution of the supply chain security plan
- Monitor performance of the supply chain security plan execution,
- Periodically reassess the state of supply chain security to detect changes in conditions including new threats,