PD ISO/PAS 28004-2:2012

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This Published Document is the UK implementation of ISO/PAS 28004-2:2012.

The UK participation in its preparation was entrusted to Technical Committee SME/32, Ships and marine technology - Steering committee.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012.

Published by BSI Standards Limited 2012.

ISBN 978 0 580 74911 7

ICS 47.020.99

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 December 2012.

Amendments issued since publication

Amd. No.	Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/PAS 28004-2:2012

PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 28004-2

First edition
2012-07-15

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

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

Partie 2: Lignes directrices pour l'adoption de l'ISO 28000 lors de l'utilisation dans les opérations portuaires petites et moyennes

Reference number
ISO/PAS 28004-2:2012(E)

Documents
Document Sharing Hub

© ISO 2012

Full document details: PD ISO/PAS 28004-2:2012

COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Documents
Document Sharing Hub
© ISO 2012 – All rights reserved

Full document details: PD ISO/PAS 28004-2:2012

Contents

Page

Foreword v

Introduction vi

1 Overview 1
1.1 Objective 1
1.2 Scope 1
1.3 Background 1
1.4 ISO 28000, 4.3.1 requirements for security risk assessment 2
1.5 Risk assessment requirements 3
1.5.1 General 3
1.5.2 Medium - small seaport risk assessment considerations 3
1.5.3 Intent 4
1.5.4 The process 4
1.5.5 Expected inputs 5
1.5.6 Expected output 5
1.5.7 Certification process 6

2 Supply chain seaport risk areas 6
2.1 General 6
2.2 Accidents - port operations 6
2.2.1 Nature of risk 6
2.2.2 Risk assessment 7
2.2.3 Mitigation strategies 7
2.2.4 Recovery guidelines 7
2.3 Criminal activity risks 7
2.3.1 Nature of risk 7
2.3.2 Risk assessment 8
2.3.3 Mitigation strategies 8
2.3.4 Recovery guidelines 9
2.4 Fire risks 9
2.4.1 Nature of risk 9
2.4.2 Risk assessment: 9
2.4.3 Mitigation strategies 10
2.4.4 Recovery guidelines 10
2.5 Stakeholder financial risks 10
2.5.1 Nature of risks 10
2.5.2 Risk assessment 11
2.5.3 Mitigation strategies 11
2.5.4 Recovery guidelines: 11
2.6 Labor related risks 11
2.6.1 Nature of risks 11
2.6.2 Risk assessment 12
2.6.3 Mitigation strategy 12
2.6.4 Recovery guidelines 12
2.7 Mechanical/equipment breakdown risks 12
2.7.1 Nature of risks 12
2.7.2 Risk assessment 13
2.7.3 Mitigation strategies 13
2.7.4 Recovery guidelines 13
2.8 Political and governmental risks 13
2.8.1 Nature of risks 13
2.8.2 Risk assessment 14
2.8.3 Mitigation strategies 14

Documents
Document Sharing Hub

© ISO 2012 – All rights reserved

Full document details: PD ISO/PAS 28004-2:2012

2.8.4 Recovery guidelines 14
2.9 Terrorist risks 15
2.9.1 Nature of risks 15
2.9.2 Risk assessment 15
2.9.3 Mitigation strategy 15
2.9.4 Recovery guidelines 16
2.10 Weather related risks 16
2.10.1 Nature of risks 16
2.10.2 Risk assessment 17
2.10.3 Mitigation strategies 17
2.10.4 Recovery guidelines 17

3 Seaport security plan evaluation criteria and rating process 18
3.1 General 18
3.2 Security plan evaluation process and procedures 18
3.3 Evaluation criteria for assessing conformance 18
3.4 Use of ISO 20858 security evaluation and assessment procedures 19
3.5 Security plan assessment rating system 20

© ISO 2012 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/PAS 28004-2:2012

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 28004-2 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*

© ISO 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/PAS 28004-2:2012

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 seaports 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.

The Medium and Small seaport 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 the seaport 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, will be undertaken.

Relationship with ISO Relevant Technical Standards

There are several established and pending related ISO technical standards that when coupled with this part of ISO/PAS 28004, provide additional guidance and instructions for the seaport operators for establishing their security management plans and evaluating the capability of those plans to protect the integrity of the supply chain cargo while under their direct control. These standards, ISO 20858, ISO 28001, ISO 28002, ISO 28003, including ISO 28004 are referenced in thispart of ISO/PAS 28004 and in order to provide specific guidance steps to Operators. The relevance of these standards to ISO 28000 is presented in the following Table.

© ISO 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/PAS 28004-2:2012

ISO Technical Standard	Technical Description
ISO 28004-1	Provides guidance to certifying bodies on assessing conformance of an organization with the requirements of ISO 28000
ISO 20858	Provides a professional interpretation of the IMO ISPS for port facility security and guidance for evaluating the Port security management plans and installed operational procedures.
ISO 28001	Provides security requirements addresses the core security requirements of the World Customs Organization (WCO) Authorized Economic Operator Program
ISO 28002	Provides guidance on establishing a policy to enhance the resilience of an organization's supply chain
ISO 28003	Provides guidance to certifying bodies on assessing conformance of an organization with the requirements of ISO 28000

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.

© ISO 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/PAS 28004-2:2012

PUBLICLY AVAILABLE SPECIFICATION ISO/PAS 28004-2:2012(E)

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

1 Overview

1.1 Objective

The objective of this part of ISO/PAS 28004 is to provide guidance to medium and small ports that wish to adopt ISO 28000. This guidance provides a self-evaluation criterion that could be used by these ports as they implement ISO 28000. While the self-certification criteria will not result in a 3rd party certification, it can be used to determine the capability of the seaport stakeholders' security management plans for safeguarding the integrity of supply chain in accordance with the security provisions and guidelines specified in ISO 28000 and ISO 28004. The goal is to develop a risk assessment evaluation rating scale metric that can be used to evaluate the capability of the port security management plans to provide uninterrupted security protection and continuous operations for the supply chain cargo being received, stored, and transferred by the seaport. The use of these self-evaluation criteria will enable the user to determine if the seaport has addressed each requirement of ISO 28000 in adequate detail.

1.2 Scope

This part of ISO/PAS 28004 will identify supply chain risk and threat scenarios, procedures for conducting risks/threat assessments, and evaluation criteria for measuring conformance and effectiveness of the documented security plans in accordance with ISO 28000/28004 implementation guidelines. An output of this effort will be a level of confidence rating system based on the quality of the security management plans and procedures implemented by the seaport to safeguard the security and ensure continuity of operations of the supply chain cargo being processed by the seaport. The rating system will be used as a means of identifying a measurable level of confidence (on a scale of 1 to 5) that the seaport security operations are in conformance with ISO 28000 for protecting the integrity of the supply chain.

1.3 Background

The International Ship and Port Facility Security (ISPS) Code requires that each maritime port facility develop a comprehensive port facility security plan that includes the cargo under their direct control. The port security plan should address those applications, security systems and operations measures designed to protect the personnel, port facilities, ships at berth, cargo, and cargo transport units, including rail and ground within the port facility physical boundaries from the risks of a security incident (ISO 20858 provides clear guidance on meeting these requirements). The ISO 28000/28004 Standard has established guidelines for protecting the Global Supply Chain at a very high level, but does not provide enough specific detail that would allow a consistent level of implementation to cover all of the security provisions and applications for large, medium and smaller seaports that are integral parts of the global supply chain security infrastructure. To ensure long term and consistent security of the supply chain, there is a need for each of the stakeholders in this integrated global network to be measured and held accountable for contributing to the safety and uninterrupted delivery of goods.

© ISO 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/PAS 28004-2:2012