BS ISO 28004-2:2014

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 British Standard is the UK implementation of ISO 28004-2:2014. It supersedes PD ISO/PAS 28004-2:2012 which is withdrawn.

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 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 77200 9

ICS 47.020.99

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2014.

**Amendments issued since publication**

| Date | Text affected |
|---|---|

Documents
Document Sharing Hub

Full document details: BS ISO 28004-2:2014

# INTERNATIONAL STANDARD

# ISO 28004-2

First edition
2014-02-01

# 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 28004-2:2014(E)

Documents
Document Sharing Hub

© ISO 2014

Full document details: BS ISO 28004-2:2014

**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested 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



© ISO 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 28004-2:2014

# Contents

Page

**Foreword** ..... **iv**

**Introduction** ..... **v**

**1 Scope** ..... **1**

**2 Overview** ..... **1**
2.1 Objective ..... 1
2.2 Background ..... 1
2.3 ISO 28000, 4.3.1 requirements for security risk assessment ..... 2
2.4 Risk assessment requirements ..... 3

**3 Supply chain seaport risk areas** ..... **6**
3.1 General ..... 6
3.2 Accidents — Port operations ..... 6
3.3 Criminal activity risks ..... 7
3.4 Fire risks ..... 9
3.5 Stakeholder financial risks ..... 10
3.6 Labour related risks ..... 12
3.7 Mechanical/equipment breakdown risks ..... 13
3.8 Political and governmental risks ..... 14
3.9 Terrorist risks ..... 15
3.10 Weather related risks ..... 17

**4 Seaport security plan evaluation criteria and rating process** ..... **18**
4.1 General ..... 18
4.2 Security plan evaluation process and procedures ..... 18
4.3 Evaluation criteria for assessing conformance ..... 19
4.4 Use of ISO 20858 security evaluation and assessment procedures ..... 20
4.5 Security plan assessment rating system ..... 20

**Bibliography** ..... **22**

© ISO 2014 – All rights reserved


Documents
Document Sharing Hub
Full document details: BS ISO 28004-2:2014

# 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 8, *Ships and marine technology*.

This first edition of ISO 28004-2 cancels and replaces ISO/PAS 28004-2:2012. It also incorporates the Amendment ISO 28004-1:2007/DAmd1.

ISO 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 1: General principles*

— *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 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 28004-2:2014

# Introduction

This part of ISO 28004 is designed to provide guidance and amplifying information for medium and small seaports desiring to adopt ISO 28000. 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 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 international standards: ISO 20858, ISO 28001, ISO 28002, ISO 28003, including the ISO 28004 series are referenced in this part of ISO 28004 and in order to provide specific guidance steps to operators. The relevance of these international standards to ISO 28000 is presented in Table 1.

**Table 1 — Relevant ISO technical standards**

| 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 |

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 28004-2:2014

Documents
Document Sharing Hub

# 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 Scope

This part of ISO 28004 identifies 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 and the ISO 28004 series 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.

## 2 Overview

### 2.1 Objective

The objective of this part of ISO 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 third 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 the ISO 28004 series. 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.

### 2.2 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). ISO 28000 and the ISO 28004 series have established guidelines for protecting the Global Supply Chain at a very high level, but do 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.

The Medium and Small seaports are an integral part of the supply chain delivery infrastructure especially considering that these ports are typically the first entry points for a majority of the goods

© ISO 2014 – All rights reserved



AVA Documents Document Sharing Hub

Full document details: BS ISO 28004-2:2014

being shipped and distributed to local and international destinations. These smaller ports are the feeder ports for goods being shipped to the larger mega ports for consolidating cargo for distribution to long haul shipment to other mega ports and global destinations. Therefore, it is critical that these Medium and Small sized seaports implement and maintain proven security provisions that can ensure the protection and continued safe passage of goods being shipped through their port facilities.

While ISO 28000 and the ISO 28004 series provide general overviews of the expected requirements to secure the supply chain, there are limited instructions, measurable requirements and acceptance criteria that would allow an entity to create and implement a security management plan that would ensure that the established standards in ISO 28000 were met. Therefore, this part of ISO 28004 is designed to provide the methods, procedures, guidelines and acceptance criteria that will be used for measuring the level of conformance with ISO 28004 security provisions.

## 2.3 ISO 28000, 4.3.1 requirements for security risk assessment

ISO 28000, 4.3.3 states "When establishing and reviewing its objectives, an organization shall take into account: a) legal, statutory and other security regulatory requirements" The ISPS Code as adopted by each member state establishes such security risk assessment requirements. Clause 4.3.1 of ISO 28000 therefore requires, the seaport stakeholders and governing organization establish and maintain procedures for the ongoing identification and assessment of security threats, security management-related threats and risks, and the identification and implementation of the necessary management control measures to safeguard the supply chain. The security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the seaport operations. This assessment shall consider the likelihood of an event and all of its consequences to the seaport stakeholders, threats to continuity of operations, supply chain security, and disaster recovery. Specifically, the risk assessment should address at a minimum, the following:

a) Operational threats and risks, including the control of the security, human factors and other activities, which affect the organizations performance, condition or safety.

b) Natural environmental events (storms, floods, high winds, etc.), which may render security measures and equipment ineffective.

c) Factors outside of the organization's control, such as failures in externally supplied equipment and services, changes in local and international security policies and regulations, and political changes affecting seaport ownership and operations.

d) Stakeholder threats and risks such as failure to meet regulatory requirements, financial constraints, or ownership changes that affect port operations and supply chain security.

e) Design, installation, validation and maintenance of security equipment including installation of new systems and training of staff to operate, repair and maintain.

f) Failure of critical information, data management and communication systems used to manage and safeguard the supply chain.

The seaport stakeholder organizations responsible for providing security protection for supply chain goods shall ensure that the results of these assessments and the appropriate security controls are in place to safeguard the integrity of the supply chain. The seaport Security Management Plan must provide provisions and procedures for addressing the security system objectives, operational requirements, risk assessment and mitigation, continuity of operations and disaster recovery steps. Specifically, the plan should address the following:

— The determination of requirements for the design, specification, installation, certification and operation of security devices and systems;

— Identification of security staffing resources, skill levels, and training needed to operate and maintain security devices and systems (ISO 28000, 4.4.2);


© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 28004-2:2014

— Identification of the organization's overall threat and risk assessment and management framework to mitigate identified risks.

— Continuity of operation provisions and disaster recovery steps that will be implemented to restore security systems for protecting the supply chain and restore the seaport to full operational status.

The organization shall document and keep the above information up to date and have personnel trained in the understanding and application of the security and operational plans and procedures specified in the plan. The organization's methodology for threat and risk identification, assessment and mitigation shall at a minimum do the following:

— Be clearly defined with respect to its scope, stakeholder roles and responsibilities, expected nature and timing of risks and threats to ensure it is proactive rather than reactive.

— Identify and the monitor the collection of information sources to document existing and determine future supply chain related security threats and risks.

— Provide for the classification of threats and risks and the identification of mitigation steps for those that must be either avoided, eliminated or controlled.

— Provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation (ISO 28000, 4.5.1) to ensure uninterrupted protection of the supply chain.

The seaport security management plan should be a planned part of the continuous improvement procedures for keeping the seaport personnel and systems current with identified threats, risks and operational security needs required to safeguard the supply chain.

The security threat identification, risk assessment and risk management processes and their outputs should be the basis for developing and implementing a comprehensive supply chain security system. It is important that the links between the security threat identification, risk assessment and risk management processes and the other elements of the security management system are clearly established, continually monitored and updated to reflect any changes in the threats and risks assessments to port operations for safeguarding the supply chain.

## 2.4 Risk assessment requirements

### 2.4.1 General

Security threat identification, risk assessment and risk mitigation processes are key tools in the management, control and elimination of risks to the security and continuous operation of the supply chain. The seaport security management plan must address each of these areas and provide specific roles and responsibilities for each stakeholder involved in safeguarding the supply chain.

### 2.4.2 Medium - small seaport risk assessment considerations

The goal of the document is to create a process for assessing the risk to the Supply Chain and what steps are in place to minimize and prevent major disruptions to the supply chain cargo being transported through the mid and small sized seaports. These seaports are usually the initial entry point for a large segment of the goods being shipped to the larger and mega international seaports. Cargo entering the ports from upstream locations via rail, truck and transport vessels that either transfer or collect cargo stored at the port locations. Therefore the goal is to determine and assess the ability of the port operations to safeguard the cargo and maintain the expected delivery pace of the products as goods past through the seaport.

The inbound collection, processing, storage, loading/unloading of cargo and final outbound shipping requirements and port operations plan and security plans that is designed to have a functional Continuity of Operations Plan (COOP) designed around the identified and perceived risks associated with the amount, flow and type of cargo being handled by the port. For each identified risk and/or threat to the flow of goods through the port must have a plan in place to either avoid, prevent or minimize the impact of the risks with work a rounds and formal disaster recover plans to provide COOP for the

© ISO 2014 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO 28004-2:2014