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)

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 28004-2 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*

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 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.

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.

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 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 28000/28004 provides 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/PAS 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.

1.4 ISO 28000, 4.3.1 requirements for security risk assessment

In accordance with the ISPS Code requirement and the security risk assessment requirements specified in 4.3.1 of ISO 28000, the seaport stakeholders and governing organization shall 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:

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

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

c) Identification of the organization’s overall threat and risk assessment and management framework to mitigate identified risks.

d) 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:

a) 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.

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

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

d) 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.

This 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.

1.5 Risk assessment requirements

1.5.1 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.

1.5.2 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 port and the flow of goods. These plans that are developed and maintained by the port operations and associated stakeholders will be evaluated and assigned a certification/level of confidence number that can be used to measure the level of conformance with the ISO 2800/28004 guidelines for protection of the supply chain.

The major output of the document will be a set of guidelines to assess the conformance of the seaport security management plans with the ISO 28004 Standards. The guidelines will cover the identification of risks and threats to the seaport operations and the documented procedures and practices implemented by the seaport stakeholders to prevent, detect, respond and restore the port to normal operational status to safeguard and ensure the continuity of operations for the supply chain.

1.5.3 Intent

The intent is to create and document a set of procedures for measuring the capability of the Medium and Small sized seaports to comply with the supply chain security requirements specified in ISO 28000 and ISO 28004 for the identified threats and risks to their seaport operations. Security threat identification, risk assessment and risk management processes are key tools in the management and reduction of security risks to supply chain operations. Security threats and risks can vary greatly across the supply chain infrastructure from minor incidents to full-scale breaches in cargo security. The goal is to (a), identify and characterize those threats and risks that are specific to the smaller seaports; determine the possible impacts to port security operations; (b), evaluate the seaport mitigation processes and prevention steps developed in response to those threats/risks; (c), and then assess the capability of the seaport to maintain the integrity of the supply chain for goods being transported through its facilities. The seaport security management plan will then be evaluated to determine the capability of the seaport to protect the supply chain against the identified threats and risks to their operations.

1.5.4 The process

Security threat identification, risk assessment and risk management processes are key tools in the management of risk. Security threat identification, risk assessment and risk management processes vary greatly across industries, ranging from simple assessments to complex quantitative analyses with extensive documentation. Therefore, the seaport Stakeholder organizations and agencies must maintain a comprehensive security management plan that addresses those threats and risks to their operations.

The seaport stakeholder organizations and agencies responsible for supply chain security, as well as port operations, are required to create and maintain a security management plan that identifies all credible threats and risks to port and security operations and creates mitigation strategies and recovery procedures for safeguarding the integrity of the supply chain. Each seaport operation will be evaluated on quality and capability of their implemented security plan to fully protect the supply chain against the identified threats and risks that it either controls or has influence over. The performance indicators that would be used to measure the capability of the seaport security protection provisions will include at a minimum the following to determine if:

- The ISO security policy and security objectives are being achieved.
- All Identified threats and risks to supply chain security are being controlled and/or mitigated, as appropriate and countermeasures have been implemented and are effective.
- Security personnel are knowledgeable and trained in the security protection, detection, mitigation and recovery procedures needed to safeguard the supply chain.
- Incident recovery and continuity of operations plans (COOP) are well established with adequate provisions for quickly restoring port security equipment and systems designed to protect the supply chain.
- Continuous improvement processes are in place to learn from any security management system failures, including security incidents and near misses.