INTERNATIONAL STANDARD

ISO 28001

First edition
2007-10-15

Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance

Systèmes de management de la sûreté pour la chaîne d'approvisionnement — Meilleures pratiques pour la mise en application de la sûreté de la chaîne d'approvisionnement, évaluations et plans — Exigences et guidage

Reference number
ISO 28001:2007(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.

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 28001 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.

This first edition of ISO 28001 cancels and replaces ISO/PAS 28001:2006, which has been technically revised.

Introduction

Security incidents against international supply chains are threats to international trade and the economic growth of trading nations. People, goods, infrastructure and equipment — including means of transport — need to be protected against security incidents and their potentially devastating effects. Such protection benefits the economy and society as a whole.

International supply chains are highly dynamic and consist of many entities and business partners. This International Standard recognizes this complexity. It has been developed to allow an individual organization in the supply chain to apply its requirements in conformance with the organization's particular business model and its role and function in the international supply chain.

This International Standard provides an option for organizations to establish and document reasonable levels of security within international supply chains and their components. It will enable such organizations to make better risk-based decisions concerning the security in those international supply chains.

This International Standard is multimodal and is intended to be in concert with and to complement the World Customs Organization's Framework of Standards to secure and facilitate global trade (Framework). It does not attempt to cover, replace or supersede individual customs agencies' supply chain security programmes and their certification and validation requirements.

The use of this International Standard will help an organization to establish adequate levels of security within those part(s) of an international supply chain which it controls. It is also a basis for determining or validating the level of existing security within such organizations' supply chain(s) by internal or external auditors or by those government agencies that choose to use compliance with this International Standard as the baseline for acceptance into their supply chain security programmes. Customers, business partners, government agencies and others might request organizations which claim compliance with this International Standard to undergo an audit or a validation to confirm such compliance. Government agencies might find it mutually agreeable to accept validations conducted by other governments' agencies. If a third-party organization audit is to be conducted, then the organization needs to consider employing a third-party certification body accredited by a competent body, which is a member of the International Accreditation Forum (see Annex C).

It is not the intention of this International Standard to duplicate governmental requirements and standards regarding supply chain security in compliance with the WCO SAFE Framework. Organizations that have already been certified or validated by mutually recognizing governments are compliant with this International Standard.

Outputs resulting from this International Standard will be the following.

— A Statement of Coverage that defines the boundaries of the supply chain that is covered by the security plan.

— A Security Assessment that documents the vulnerabilities of the supply chain to defined security threat scenarios. It also describes the impacts that can reasonably be expected from each of the potential security threat scenarios.

— A Security Plan that describes security measures in place to manage the security threat scenarios identified by the Security assessment.

— A training programme setting out how security personnel will be trained to meet their assigned security related duties.

To undertake the security assessment needed to produce the security plan, an organization using this International Standard will

— identify the threats posed (security threat scenarios);

— determine how likely persons could progress each of the security threat scenarios identified by the Security Assessment into a security incident.

This determination is made by reviewing the current state of security in the supply chain. Based on the findings of that review, professional judgment is used to identify how vulnerable the supply chain is to each security threat scenario.

If the supply chain is considered unacceptably vulnerable to a security threat scenario, the organization will develop additional procedures or operational changes to lower likelihood, consequence or both. These are called countermeasures. Based upon a system of priorities, countermeasures need to be incorporated into the security plan to reduce the threat to an acceptable level.

Annexes A and B are illustrative examples of risk management based security processes for protecting people, assets and international supply chain missions. They facilitate both a macro approach for complex supply chains and/or more discrete approaches for portions thereof.

These annexes are also intended to

— facilitate understanding, adoption and implementation of methodologies, which can be customized by organizations;

— provide guidance for baseline security management for continual improvement;

— assist organizations to manage resources to address existing and emerging security risks;

— describe possible means for assessment of risk and mitigation of security threats in the supply chain from raw materiel allocation through storage, manufacturing and transportation of finished goods to the market place.

Annex C provides guidance for obtaining advice and certification for this International Standard if an organization using it chooses to exercise this option.

Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance

1 Scope

This International Standard provides requirements and guidance for organizations in international supply chains to

- develop and implement supply chain security processes;
- establish and document a minimum level of security within a supply chain(s) or segment of a supply chain;
- assist in meeting the applicable authorized economic operator (AEO) criteria set forth in the World Customs Organization Framework of Standards and conforming national supply chain security programmes.

NOTE Only a participating National Customs Agency can designate organizations as AEOs in accordance with its supply chain security programme and its attendant certification and validation requirements.

In addition, this International Standard establishes certain documentation requirements that would permit verification.

Users of this International Standard will

- define the portion of an international supply chain within which they have established security (see 4.1);
- conduct security assessments on that portion of the supply chain and develop adequate countermeasures;
- develop and implement a supply chain security plan;
- train security personnel in their security related duties.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 20858:—[1)], *Ships and marine technology — Maritime port facility security assessments and security plan development*

1) To be published. Revision of ISO/PAS 20858:2004.

International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, International Maritime Organization

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
appropriate law enforcement and other government officials
those government and law enforcement personnel that have specific legal jurisdiction over the international supply chain or portions of it

3.2
asset(s)
plant, machinery, property, buildings, vehicles, ships, aircraft, conveyances 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 information system that is integral to the delivery of security and the application of security management.

3.3
authorized economic operator
party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national customs administration as complying with WCO or equivalent supply chain security standards

NOTE 1 Authorized economic operator is a term defined in the World Customs Organization Framework of Standards.

NOTE 2 Authorized economic operators include *inter alia* manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses and distributors.

3.4
business partner
those contractors, suppliers or service providers that an organization contracts with to assist the organization in its function as an **organization in the supply chain** (3.15)

3.5
cargo transport unit
road freight vehicle, railway freight wagon, freight container, road tank vehicle, railway tank wagon or portable tank

3.6
consequence
loss of life, damage to property or economic disruption, including disruption to transport systems, that can reasonably be expected as a result of an attack on an organization in the supply chain or by the use of the supply chain as a weapon

3.7
conveyance
physical instrument of international trade that transports goods from one location to another

EXAMPLES Box, pallet, cargo transport unit, cargo handling equipment, truck, ship, aircraft and railcar.

3.8
countermeasures
actions taken to lower the likelihood of a security threat scenario succeeding in its objectives, or to reduce the likely consequences of a security threat scenario

3.9
custody
period of time where an organization in the supply chain is directly controlling the manufacturing, processing, handling and transportation of goods and their related shipping information within the supply chain

3.10
downstream
handling, processes and movements of goods when they no longer are in the custody of the organization in the supply chain

3.11
goods
those items or materials that, upon the placement of a purchase order, are being manufactured, processed, handled or transported within the supply chain for usage or consumption by the purchaser

3.12
international supply chain
supply chain that at some point crosses an international or economic border

NOTE 1 All portions of this chain are considered international from the time a purchase order is concluded to the point where the goods are released from customs control in the destination country or economy.

NOTE 2 If treaties or regional agreements have eliminated customs clearance of goods from specified countries or economies, the end of the international supply chain is the port of entry into the destination country or economy where the goods would have cleared customs if the agreements or treaties had not been in place.

3.13
likelihood
ease or difficulty with which a security threat scenario could progress to become a security incident

NOTE Likelihood is evaluated based on the resistance the security processes in place pose to a security incident involving the security threat scenario being examined and is expressed either qualitatively or quantitatively.

3.14
management system
organization's structure for managing its processes or activities that transform inputs of resources into a product or service, which meet the organization's objectives

NOTE It is not the intent of this International Standard to specify a specific management system or require the creation of a separate security management system. ISO 9001 (Quality Management Systems), ISO 14001 (Environmental Management Systems), ISO 28000 (Security management systems for the supply chain), and the International Maritime Organization's International Safety Management (ISM) Code are examples of management systems.

3.15
organization in the supply chain
any entity that

— manufactures, handles, processes, loads, consolidates, unloads or receives goods upon placement of a purchase order that at some point cross an international or economy border;

— transports goods by any mode in the international supply chain regardless of whether their particular segment of the supply chain crosses national (or economy) boundaries; or

— provides, manages or conducts the generation, distribution or flow of shipping information used by customs agencies or in business practices.

3.16
risk management
process of making management decisions based on an analysis of possible threats, their consequences, and their probability or likelihood of success

NOTE A risk management process is normally initiated for the purposes of optimizing the organization's resource allocation necessary to operate in a particular environment.

3.17
scope of service
function(s) that an organization in the supply chain performs, and where it performs this/these functions

3.18
security declaration
documented commitment by a business partner, which specifies security measures implemented by that business partner, including, at a minimum, how goods and physical instruments of international trade are safeguarded, associated information is protected and security measures are demonstrated and verified

NOTE It will be used by the organization in the supply chain to evaluate the adequacy of security measures related to the security of goods.

3.19
security plan
planned arrangements for ensuring that security is adequately managed

NOTE 1 It is designed to ensure the application of measures that protect the organization from a security incident.

NOTE 2 The plan can be incorporated into other operational plans.

3.20
security
resistance to intentional acts designed to cause harm or damage to or by the supply chain

3.21
security incident
any act or circumstance that produces a **consequence** (3.6)

3.22
security personnel
those people in the organization in the supply chain that have been assigned security related duties

NOTE These people may or may not be employees of the organization.

3.23
security sensitive information
security sensitive materials
information or materials, produced by or incorporated into the supply chain security process, that contain information about the security processes, shipments or government directives that would not be readily available to the public and would be useful to someone wishing to initiate a security incident

3.24
supply chain
linked set of resources and processes that upon placement of a purchase order begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of goods and related services to the purchaser

NOTE The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centres, distributors, wholesalers and other entities involved in the manufacturing, processing, handling and delivery of the goods and their related services.

3.25
target
personnel, means of transport, goods, physical assets, manufacturing processes and handling, control or documentation systems within an organization in the supply chain

3.26
security threat scenario
means by which a potential security incident might occur

3.27
upstream
handling, processes and movements of goods that occur before the organization in the supply chain takes custody of the goods

3.28
World Customs Organization
WCO
independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of customs administrations

NOTE It is the only intergovernmental worldwide organization competent in customs matters.

4 Field of application

4.1 Statement of application

The organization in the supply chain shall describe the portion of the international supply chain that it claims to be in compliance with this International Standard in a Statement of Application. The Statement of Application shall at least include the following information:

a) details of the organization;

b) scope of service;

c) names and contact information of all business partners within the defined scope of service;

d) date the security assessment was completed and period of validity of the security assessment; and

e) signature of an individual authorized to sign on behalf of that organization.

Organizations in the supply chain may extend the Statement of Application to include other parts of the supply chain, e.g. including final destination.

4.2 Business partners

If within the supply chain described in the Statement of Application the organization is using business partners, the organization shall, subject to 4.3 and 4.4, require such business partners to provide a security declaration. The organization shall consider this security declaration in its security assessment and may require specific countermeasures to be enacted.

4.3 Internationally accepted certificates or approvals

Transportation companies and facilities, which hold internationally accepted certificates or approvals, issued pursuant to mandatory international conventions governing the security of the various transportation sectors, will have in place security practices, plans and processes that meet the applicable requirements of this International Standard and are not required to be audited to confirm such compliance. For shipping companies, ships and port facilities, the certificates or approvals shall be issued in accordance with SOLAS XI-2/4 or SOLAS XI-2/10, as applicable.

In conformance with Clause 1, national customs agencies may, in addition to possession of internationally accepted security certificates or approvals, require additional security measures and practices to be implemented by transportation companies and facilities as a condition for designation as an AEO.

4.4 Business partners exempt from security declaration requirement

Those business partners that confirm to the organization that they

a) are verified compliant with this International Standard or ISO 20858,

b) are covered by 4.3, or

c) have been designated as AEOs in accordance with a national customs agency's supply chain security programme which has been determined to be in accordance with the WCO SAFE Framework,

shall be listed on the Statement of Application. However, the organization does not need to conduct additional security assessments for such business partners or require them to provide security declarations.

4.5 Security reviews of business partners

Except for business partners covered by 4.3 or 4.4, the organization in the supply chain shall conduct reviews of their business partners' processes and facilities to ascertain the validity of their declarations of security. The extent and the frequency of these reviews shall be determined through an analysis of the risks involved. The organization shall maintain results of these reviews.

NOTE To provide for ease of reading the organization claiming compliance, including those parts of its supply chain operated by business partners, whether compliant with this International Standard or not, is in the ensuing paragraphs referred to as the "organization" unless clarity demands otherwise.

5 Supply chain security process

5.1 General

Organizations in international supply chains that have adopted this International Standard are required both to manage security throughout their portion of the supply chain and to have a management system in place in support of that objective. This International Standard requires security practices and/or processes to be established and implemented in order to reduce the risk to the international supply chain from activities that could lead to a security incident.

Organizations in the supply chain claiming compliance with this International Standard shall have a security plan based on the output from the security assessment that documents existing security measures and procedures and incorporates countermeasures as applicable for the portion of the international supply chain that they have included in their Statement of Application.

5.2 Identification of the scope of the security assessment

The scope of the security assessment shall include all activities performed by the organization as described in its Statement of Application (see 4.1). The assessment shall be periodically performed and the security plan shall be revised as appropriate. The results of the assessment shall be documented and retained.

The security assessment shall also cover information systems, documents and networks pertaining to the handling and movement of the goods while in the custody of the organization. Existing security arrangements shall, subject to 4.3 and 4.4, be assessed at all locations and for business partners where there are potential security vulnerabilities.