

PUBLICLY
AVAILABLE
SPECIFICATION

**ISO/PAS
28001**

First edition
2006-09-01

**Security management systems for
the supply chain — Best practices for
implementing supply chain security —
Assessments and plans**

*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*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/PAS 28001:2006](https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-17c5dc05243a/iso-pas-28001-2006)

<https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-17c5dc05243a/iso-pas-28001-2006>



Reference number
ISO/PAS 28001:2006(E)

© ISO 2006

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/PAS 28001:2006](https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-17c5dc05243a/iso-pas-28001-2006)

<https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-17c5dc05243a/iso-pas-28001-2006>

© ISO 2006

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

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	2
4 Field of application	5
4.1 Statement of application	5
4.2 Business partners.....	5
4.3 Internationally accepted certificates or approvals	5
4.4 Business partners exempt from security declaration requirement.....	6
4.5 Security reviews of business partners	6
5 Supply chain security process	6
5.1 General.....	6
5.2 Identification of the scope of security assessment	6
5.3 Conduction of the security assessment.....	7
5.4 Development of the supply chain security plan	8
5.5 Execution of the supply chain security plan	8
5.6 Documentation and monitoring of the supply chain security process.....	8
5.7 Actions required after a security incident.....	8
5.8 Protection of the security information	8
Annex A (informative) Supply chain security process	10
Annex B (informative) Methodology for security risk assessment and development of countermeasures.....	18
Annex C (informative) Guidance for obtaining advice and certification	26
Bibliography	27

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 normative 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 28001 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 11, *Intermodal and short sea shipping*.

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, should 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 Publicly Available Specification 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 Publicly Available Specification is 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 Publicly Available Specification 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.

This Publicly Available Specification is a voluntary specification to help organizations to establish adequate levels of security within those part(s) of an international supply chain which they control. 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 Publicly Available Specification as the baseline for acceptance into their supply chain security programmes. Customers, business partners, government agencies and others may request organizations which claim compliance with this Publicly Available Specification to undergo an audit or a validation to confirm such compliance. Government agencies may 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 should 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 Publicly Available Specification to duplicate governmental requirements and standards regarding supply chain security in compliance with the WCO Framework. Organizations that have already been certified or validated by mutually recognizing governments are compliant with this Publicly Available Specification.

Outputs resulting from this document 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 scenarios. It also describes the impacts expected from each of the potential threat scenarios.
- A Security Plan that describes security measures in place to manage the security threats identified by the Security assessment.
- A training programme setting out how security personnel will be trained to meet their assigned security related duties.

ISO/PAS 28001:2006(E)

To undertake the security assessment needed to produce the security plan, an organization using this Publicly Available Specification will

- identify the threats posed (security scenarios);
- determine how likely persons could carry out each of the security scenarios identified by the Security Assessment.

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

If the supply chain is considered unacceptably vulnerable to a security 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 should 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 risk 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 material allocation through storage, manufacturing, and transportation of finished goods to the market place.

Annex C provides guidance for obtaining advice and certification for ISO/PAS 28001 if an organization using this Publicly Available Specification chooses to exercise this option.

Security management systems for the supply chain — Best practices for implementing supply chain security — Assessments and plans

1 Scope

This Publicly Available Specification 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 Operators 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 Authorized Economic Operators in accordance with its supply chain security programme and its attendant certification and validation requirements.

In addition, this Publicly Available Specification establishes certain documentation requirements that would permit verification.

[ISO/PAS 28001:2006](https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-17c3d03245/iso-pas-28001-2006)

[https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-](https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-17c3d03245/iso-pas-28001-2006)

Users of this Publicly Available Specification will <https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-17c3d03245/iso-pas-28001-2006>

- define the portion of an international supply chain they have established security within (see 4.1);
- conduct security vulnerability 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 may be required 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/PAS 20858, *Ships and marine technology — Maritime port facility security assessments and security plan development*

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
contractor, supplier or service provider that an organization contracts with to assist the organization in its function as an organization in the supply chain

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
likely loss of life, damage to property or economic disruption, including disruption to transport systems, caused by 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 countermeasure
action 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 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 things that upon the placement of a purchase order are manufactured, processed, handled and 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 economy border

NOTE 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. 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 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 Publicly Available Specification to require either a specific management system and/or the creation of a separate security management system. ISO 9001 (Quality Management Systems), ISO 14001 (Environmental Management Systems), ISO/PAS 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 threatens the security of a target

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.22

security personnel

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

ISO/PAS 28001:2006

<https://standards.iteh.ai/catalog/standards/sist/5367b-c871-4716-8101-17c5dc05243a/iso-pas-28001-2006>

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

security management

systematic and coordinated activities and practices through which an organization in the supply chain manages its risks and the associated potential threats and impacts

3.25

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.

3.26

target

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

3.27**threat scenario**

means by which a potential security incident might occur

3.28**upstream**

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

3.29**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 Publicly Available Specification in a Statement of Application. The Statement of Application shall at least include the following information.

- Details of the organization.
- Scope of service.
- Names and contact information of all business partners within the defined scope of service.
- Date the security assessment was completed and period of validity of the security assessment.
- 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 the organization in the supply chain is using business partners within the portion of the international supply chain, 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 Publicly Available Specification 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 Authorized Economic Operator (AEO).

4.4 Business partners exempt from security declaration requirement

Those business partners that confirm to the organization that they

- 1) are verified compliant with this Publicly Available Specification or ISO/PAS 20858, or
- 2) are covered by 4.3, or
- 3) 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 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. Such reviews and the frequency of these reviews shall be conducted taking account of the organization's risk analysis of these business partners. 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 Publicly Available Specification or not, is in the ensuing paragraphs referred to as the "organization" unless clarity demands otherwise.

5 Supply chain security process

<https://standards.iteh.ai/catalog/standards/sist/4e53fa7b-e871-4740-8dcd-17c5dc05243a/iso-pas-28001-2006>

5.1 General

Organizations in international supply chains that have adopted this Publicly Available Specification 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 Publicly Available Specification 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 Publicly Available Specification 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 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.