
**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*

STANDARDSISO.COM : Click to view the full PDF of ISO 28001:2007



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.

STANDARDSISO.COM : Click to view the full PDF of ISO 28001 :2007



COPYRIGHT PROTECTED DOCUMENT

© ISO 2007

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.....	9
Annex A (informative) Supply chain security process	10
A.1 General.....	10
A.2 Identification of the scope of the security assessment.....	10
A.3 Conduction of the security assessment.....	11
A.4 Development of the security plan	15
A.5 Execution of the security plan.....	17
A.6 Documentation and monitoring of the security process	17
A.7 Continual improvement.....	17
Annex B (informative) Methodology for security risk assessment and development of countermeasures	18
B.1 General.....	18
B.2 Step one – Consideration of the security threat scenarios.....	20
B.3 Step two – Classification of consequences.....	22
B.4 Step three – Classification of likelihood of security incidents	23
B.5 Step four – Security incident scoring	24
B.6 Step five – Development of countermeasures.....	24
B.7 Step six – Implementation of countermeasures	25
B.8 Step seven – Evaluation of countermeasures	25
B.9 Step eight – Repetition of the process	25
B.10 Continuation of the process	25
Annex C (informative) Guidance for obtaining advice and certification	26
C.1 General.....	26
C.2 Demonstrating conformance with ISO 28001 by audit	26
C.3 Certification of ISO 28001 by third party certification bodies	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.

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 28001:2007

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.

ISO 28001:2007(E)

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 material 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.

5.3 Conduction of the security assessment

5.3.1 Assessment personnel

The person or team conducting the security assessment shall collectively have skills and knowledge which include, but are not limited to, the following:

- risk assessment techniques applicable to all aspects of the international supply chain from the point where the organization in the supply chain takes custody of the goods in to the point where the goods are no longer in the organization's custody or leaves the international supply chain;
- applying appropriate measures to avoid unauthorized disclosure of, or access to, security sensitive material;
- operations and procedures involved in the manufacturing, handling, processing, movement and/or documentation of goods as appropriate;
- security measures related to consignment, conveyance, personnel, premises, and information systems in that applicable portion of the supply chain;
- an understanding of security threats and mitigation methodologies;
- understanding of this International Standard.

The name(s) of the person or team members conducting the assessment as well as their qualifications shall be documented.

5.3.2 Assessment process

The organization shall establish, implement and maintain (a) procedure(s) to identify existing countermeasures to mitigate security threats. The organization shall list applicable security threat scenarios, including those deemed necessary by appropriate government officials. If government officials have not participated, this shall be documented in the security assessment.

For each security threat scenario, the organization shall evaluate the existing countermeasures and determine likelihood and consequence relevant to each security threat scenario and evaluate the necessity of additional countermeasures to reduce the security risk to an acceptable level.

The organization shall review the security declaration(s) provided by each business partner, defined in 4.2, and apply professional judgment, knowledge of the entity(ies) and/or requirements of regulatory agencies. It may also obtain and use any other available information, in determining the acceptance of the security declaration.

Organizations shall consider both the detail and validity of each security declaration when conducting the security assessment and determining the overall vulnerability of the supply chain described in its Statement of Application.

Business partners that are covered by 4.3 or 4.4 should not need to be assessed further.

The following information shall be documented:

- a) all security threat scenarios considered;
- b) processes used in evaluating those threats; and
- c) all countermeasures identified and prioritized.

5.4 Development of the supply chain security plan

Organizations shall develop and maintain a security plan for the entire portion of the supply chain described in their Statement of Application. The plan may be separated into annexes in which each describes the security in place for a particular segment of the supply chain, including security measures that the organizations' business partners, subject to 4.3 or 4.4, will maintain according to their security declarations. The plan/annexes shall also specify how the organization would monitor or periodically review such security declarations.

Organizations shall review and consider the use of the guidance in informative Annexes A and B when developing their security plans.

5.5 Execution of the supply chain security plan

The organization shall establish a management system to enable its specific supply chain security processes to be implemented.

5.6 Documentation and monitoring of the supply chain security process

5.6.1 General

The organization shall establish and maintain procedures to document, monitor and measure the performance of its management system referred to above. The organization shall carry out audits of the management system at planned intervals to ensure it has been properly implemented and maintained. The results of audits shall be documented and retained.

5.6.2 Continual improvement

The organization shall assess opportunities for improving its security arrangements as a means of enhancing the security of its portion of the supply chain.

5.7 Actions required after a security incident

The organization shall carry out a review of its security plan after the occurrence of any security incident that relates to any portion of the international supply chain the organization controls. This review shall

- a) determine the cause of the incident and the corrective action;
- b) determine the effectiveness of measures and procedures for security recovery; and
- c) considering such determinations, re-assess those portions of the supply chain according to 5.3.2.

In the event of a security breach, the organization shall follow reporting procedures to Customs and/or appropriate law enforcement agencies as appropriate, and as specified in the security plan and contractual relationships.

The organization shall retain consignment and other required supply chain data within the time limits prescribed in applicable laws and regulations.

5.8 Protection of the security information

Security plans, measures, processes, procedures and records of the organization shall be considered sensitive security information and protected from unauthorized access or disclosure. Such information shall only be disclosed to individuals who have a “need to know”. In addition to appropriate law enforcement officials or their nominees, an individual has a “need to know” when

- a) the individual requires access to specific sensitive security information to carry out security activities covered by the security plan;
- b) the individual is in training to carry out activities covered by the security plan;
- c) the information is necessary for the individual to supervise others carrying out security activities covered in the security plan; or
- d) the individual is, or is acting on behalf of a party, who according to a contractual relationship with the organization has been granted access to security sensitive information controlled by the organization in accordance with agreed terms and conditions.

NOTE If the organization is certified compliant with ISO 28001 by a third party certification body accredited by a competent accreditation body or has been certified or validated compliant with ISO 28001 by mutually recognizing governments, such contractually agreed access to the organization's security sensitive information may not be deemed necessary, and would in any event be dependent on the organization's explicit concurrence. The fact that its sensitive security information is protected from unauthorized access or disclosure does not prevent the organization from briefing business partners and others about its supply chain security arrangements and systems.

Annex A
(informative)

Supply chain security process

A.1 General

This annex provides guidance on the development of a supply chain security process that can be implemented in an organization with an existing management system. Figure A.1 provides a graphical description of such a process.

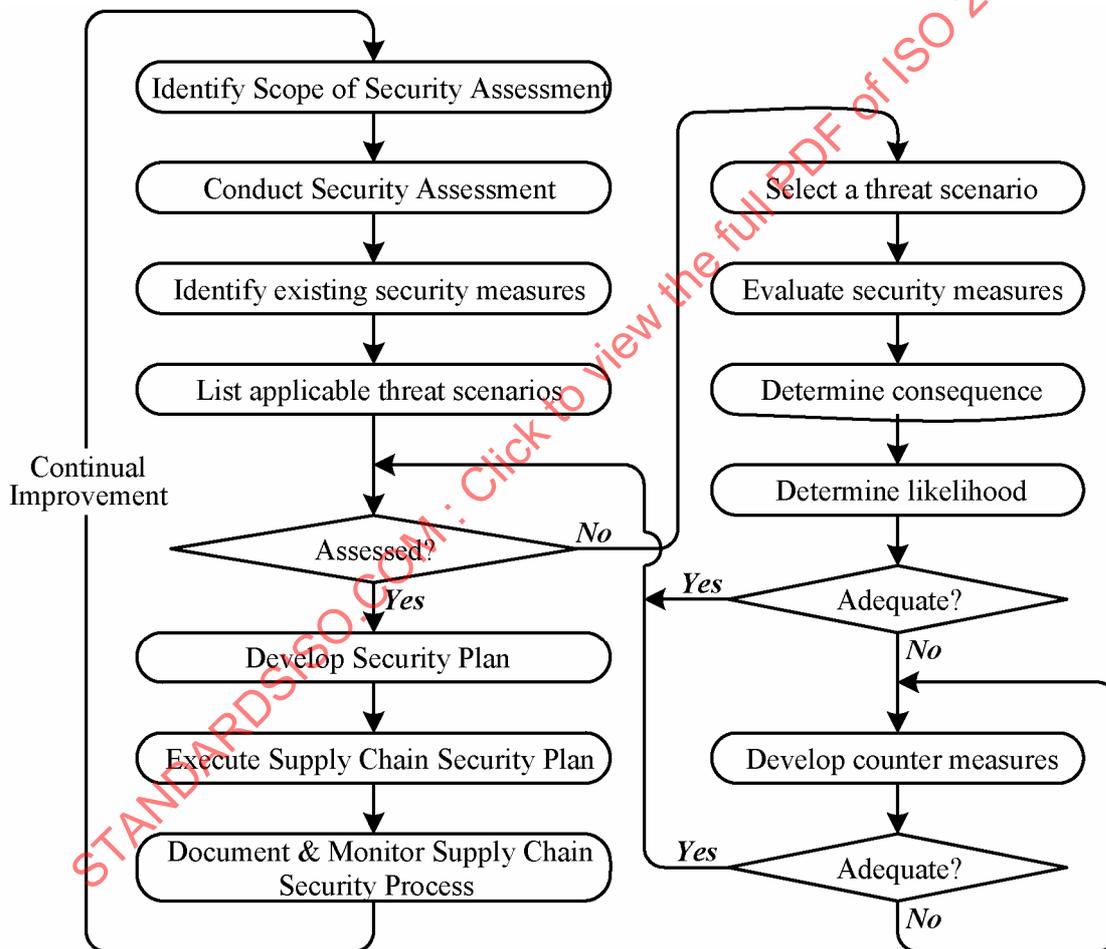


Figure A.1 — Graphical description of a supply chain security process

A.2 Identification of the scope of the security assessment

A security assessment is an attempt to identify security risks present in that part of the supply chain the organization, in accordance with its Statement of Application, desires to bring into compliance with this International Standard. To accomplish this assessment the boundaries of the scope of coverage (both physically and virtually) need to be established.

A.3 Conduction of the security assessment

A.3.1 General

Using qualified personnel the existing security arrangements at all locations has to be assessed where there are potential security vulnerabilities, which should include but are not limited to the following:

- where goods are being manufactured, processed or handled prior to being loaded in a transport unit, palletized, or otherwise prepared for shipment;
- where goods prepared for shipment are stored or consolidated prior to transportation;
- where goods are being transported;
- where goods are loaded into or unloaded from a conveyance;
- where custody of the goods changes hands;
- where documentation or information pertaining to goods being shipped is handled, generated or accessible;
- inland transportation routes and means of conveyance used by the various modes of transportation;
- other.

A.3.2 Performance review list

The following performance review list provides an example of a systematic approach for reviewing existing security arrangements.

Those portions of the performance review list that pertain to business partners, who have confirmed to the organization that they

- a) are verified compliant with this International Standard or with 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,

should contain a comment indicating how the factor has been addressed, e.g. compliant with this International Standard, ISO 20858, or the ISPS Code.

A.3.3 Performance review

The following performance review list shown in Table A.1 can be completed and considered when conducting a security assessment for an organization in the supply chain. This list is not all-inclusive, and can be tailored to reflect the risk assessment and business model of the organization. If the factor indicated is already implemented by the organization in the supply chain the "Yes" block should be checked. If the factor is not already implemented or is partially met the "No" block should be checked and, where applicable, an explanation added to the comment column describing other alternative measures utilized, or that the risk is very low. If the factor is not applicable or is outside the organization's statement of coverage, Not Applicable (NA) should be noted in the "Comments" block. Items on the performance review list that cannot be performed due to applicable laws/regulations should be marked as prohibited in the comment column.

Table A.1 — Performance review list

Factor	Yes	No	Comments
Management of Supply Chain Security			
• Does the organization have a management system that addresses supply chain security?			
• Does the organization have a person designated as responsible for supply chain security?			
Security Plan			
• Does the organization have (a) current security plan(s)?			
• Does the plan address the organization's security expectations of upstream and downstream business partners?			
• Does the organization have a crisis management, business continuity, and security recovery plan?			
Asset Security			
<ul style="list-style-type: none"> • Does the organization have in place measures that addresses <ul style="list-style-type: none"> — the physical security of buildings, — monitoring and controlling of exterior and interior perimeters, — application of access controls that prohibit unauthorized access to facilities, conveyances, loading docks and cargo areas, and managerial control over the issuance of identification (employee, visitor, vendor, etc.) and other access devices? • Are there operational security technologies which significantly enhance asset protection? For example, intrusion detection, or recorded CCTV/DVS cameras that cover areas of importance to the supply chain activity, with the recordings maintained for a long enough period of time to be of use in an incident investigation. 			
• Are there protocols in place to contact internal security personnel or external law enforcement in case of security breach?			
• Are procedures in place to restrict, detect, and report unauthorized access to all cargo and conveyance storage areas?			
• Are persons delivering or receiving cargo identified before cargo is received or released?			
Personnel Security			
• Does the organization have procedures to evaluate the integrity of employees prior to employment and periodically relative to their security duties?			
• Does the organization conduct specific job appropriate training to assist employees in performing their security duties for example: maintaining cargo integrity, recognizing potential internal threats to security and protecting access controls?			
• Does the organization make employees aware of the procedures the company has in place to report suspicious incidents?			
• Does the access control system incorporate immediate removal of a terminated employee's company-issued identification and access to sensitive areas and information systems?			

Factor	Yes	No	Comments
Information Security			
• Are procedures employed to ensure that all information used for cargo processing, both electronic and manual, is legible, timely, accurate, and protected against alteration, loss or introduction of erroneous data?			
• Does an organization shipping or receiving cargo reconcile the cargo with the appropriate shipping documentation?			
• Does the organization ensure that cargo information received from business partners is reported accurately and in a timely manner?			
• Is relevant data protected through use of storage systems not contingent on the operation of the primary data handling system (is there a data back up process in place)?			
• Do all users have a unique identifier (user ID) for their personal and sole use, to ensure that their activities can be traced to them?			
• Is an effective password management system employed to authenticate users and are users required to change their passwords at least annually?			
• Is there protection against unauthorized access to and misuse of information?			
Goods and Conveyance Security			
• Are procedures in place to restrict, detect, and report unauthorized access to all shipping, loading dock areas and closed cargo transport unit storage?			
• Are qualified persons designated to supervise cargo operations?			
• Are procedures in place for notifying appropriate law enforcement in cases where anomalies or illegal activities are detected or suspected by the organization?			
• Are procedures in place to ensure the integrity of the goods/cargo when the goods/cargo are delivered to another organization (transportation provider, consolidation centre, intermodal facility, etc.) in the supply chain?			
• Are processes in place to track changes in threat levels along transport routes?			
• Are there security rules, procedures or guidance provided to conveyance operators (for example, the avoidance of dangerous routes)?			
Closed Cargo Transport Units			
(WCO SAFE Framework includes a “Seal Integrity Program” described in the Appendix to Annex 1 that sets out procedures regarding the affixing and verification of high security seals and /or other tamper detection devices. Personnel filling in this form should review that section of the Framework).			
• If a closed cargo transport unit is used, are there documented procedures for affixing and recording high security mechanical seals meeting ISO/PAS 17712 and/or other tamper-detection devices by the party stuffing the cargo unit?			
• If a sealed closed cargo transport unit is used, are there documented procedures in place to inspect seals for signs of tampering when the custody of conveyances changes during the course of a shipment and to address detected discrepancies?			

Factor	Yes	No	Comments
<ul style="list-style-type: none"> If a closed cargo transport unit is used, is it inspected for contamination by the party stuffing immediately before stuffing? 			
<ul style="list-style-type: none"> If closed cargo transport units are used, are documented procedures in place for inspecting them immediately before stuffing by the party stuffing them to verify their physical integrity, to include the reliability of the unit locking mechanisms? A seven-point inspection process is recommended: <ul style="list-style-type: none"> — Front wall — Left side — Right side — Floor — Ceiling/Roof — Inside/outside closure — Outside/Undercarriage 			

A.3.4 Security threat scenarios

During the security assessment consider security threat scenarios, including but not limited to those listed in Table A.2. The security assessment should also consider other scenarios that may be determined by government authorities, the organization’s management or the security professional(s) conducting the assessment.

Table A.2 — Security threat scenarios to the supply chain

Security threat scenarios	Application
1 Intrude and/or take control of an asset (including conveyances) within the supply chain	Damage/destroy an asset (including conveyances). Damage/destroy outside target using the asset or goods. Cause civil or economic disturbance. Take hostages/kill people.
2 Use the supply chain as a means of smuggling	Illegal weapons into or out of the country/economy. Terrorist into or out of the country/economy.
3 Information tampering	Locally or remotely gaining access the supply chain's information/documentation systems for the purpose of disrupting operations or facilitating illegal activities.
4 Cargo Integrity	Tampering, sabotage and/or theft for the purpose of terrorism.
5 Unauthorized use	Conducting operations in the international supply chain to facilitate a terrorist incident including using the mode of transportation as a weapon.
6 Other	

A.4 Development of the security plan

A.4.1 General

The security plan and/or annexes may be incorporated into operational plans or procedures and need not be stand-alone documents. If the security plan is incorporated into other plans the organization should maintain a cross-reference table to enable verification that all the security plan requirements have been met.

The plan may be separated into annexes in which each describes the security in place for a particular segment of the supply chain, including security measures that their business partners will maintain according to their security declarations (if applicable). The plan/annexes should also specify how the organization would monitor or periodically review their security declarations. The security plan/annex should include, but should not be limited to, descriptions of the following.

- The portion of the supply chain that is covered by the plan or annex.
- The security-related duties of all security personnel.
- The security management structure including the name of the person designated as manager of security.
- Internal and external emergency security contact information to be used by personnel in reporting a security incident.
- The skills and knowledge that personnel with security responsibilities are required to possess.
- Security training programmes.
- The qualification process for people assigned security duties that ensures they possess the necessary skills and knowledge to perform their security duties.
- How elements of the security plan are exercised. Participation in government run security drills or exercises by organization personnel can be used to meet these requirements.
- Processes to meet, at a minimum, security requirements imposed by government for contingencies or heightened security levels.

The security plan should contain procedures including but not limited to the arrangements that do the following.

- Ensure that information on a shipment of goods is received before the goods being shipped are accepted by the organization for further transportation.
- Ensure goods/cargoes received for consolidation/deconsolidation are accurately reconciled against information on goods/cargo manifests/lists. Departing goods/cargo units should be verified against purchase or delivery orders.
- Ensure drivers delivering or receiving goods/cargo are positively identified before goods or cargo units are received or released.
- Ensure occupants of vehicles other than drivers are positively identified.
- Ensure all shortages, overages, and other significant discrepancies or anomalies are resolved and/or investigated appropriately and appropriate law enforcement agencies be notified if illegal or suspicious activities are detected as appropriate.
- Describe any countermeasures that have been implemented in that portion of the supply chain.
- Describe any measures and procedures that have been implemented in that portion of the supply chain for security recovery in the event of a security incident.

- Describe any measures and procedures that have been implemented when custody of the goods/cargo is transferred to another organization.
- Describe procedures for releasing additional information on the goods being shipped to authorized personnel. This should include both how the user will determine if the request for additional information is legitimate and how/what information is released.
- Describe procedures established according to A.4.3.

A.4.2 Documentation

The organization should maintain the most recent documentation of the following at a secure retrievable location.

- Statements of coverage.
- The completed security assessment.
- Names and qualifications of the personnel conducting the security assessment.
- Listing of all countermeasures that were considered.
- Security declarations.
- Security plan and, if applicable, annexes.
- Records of training sessions and exercises conducted, personnel who attended, subjects trained, and date(s).
- Other as prescribed by regulation or management.

A.4.3 Communication

The organization should where practicable establish contact with appropriate law enforcement and other government officials for the purposes of the following.

- Establishing procedures to be followed in the event of or suspicion of goods/cargo tampering, emergencies related to, or the receipt of threats concerning the international supply chain. These procedures should, if provided, include specific telephone numbers to be called at the appropriate government agencies. These procedures should be incorporated into the organization's supply chain security plan.
- Participating in consultations lead by appropriate government officials at both the national and local levels (as appropriate) to discuss matters of mutual interest including custom regulations and procedures and requirements for premise and consignment security.
- Being responsive to government outreach efforts and to contribute to a dialog that provides meaningful insight to ensure that the organizations security plan remains relevant and effective.

If the appropriate law enforcement and other government officials do not wish to participate in such a dialog, the organization should document their attempt(s) and state that appropriate law enforcement and other government officials did not participate at that time.

A.5 Execution of the security plan

The implementation of the new or revised security plan represents a change to operational practices and needs to be undertaken in accordance with the organization's management system to ensure that adequate resources are available, the impact on other operations is managed and the effectiveness of the plan is monitored and evaluated.

A.6 Documentation and monitoring of the security process

The organization should establish and maintain procedures to monitor and measure the performance of its security management system to ensure its continuing suitability, adequacy and effectiveness. The organization should consider the associated security threats and risks, including potential deterioration mechanisms and their consequences, when setting the frequency for measuring and monitoring the key performance parameters.

A.7 Continual improvement

Management in operational control of that portion of the supply chain should review the organization's security management system to assess opportunities for improvement and the need for changes to the security management system.

STANDARDSISO.COM : Click to view the full PDF of ISO 28001:2007

Annex B (informative)

Methodology for security risk assessment and development of countermeasures

B.1 General

This annex gives a methodology that may be used by organizations in international supply chains to make an assessment of the risk that their operations may suffer from security incidents, to determine the appropriate countermeasures, effective for the type and size of their supply chain operations. This methodology uses the following sequence.

- a) List all activities as covered in the Scope.
- b) Identify security controls presently in place.
- c) Identify security threat scenarios.
- d) Determine consequences if the security threat scenario was completed.
- e) What is the likelihood of this happening considering current security.
- f) Are control security measures adequate.
- g) If not develop additional security measures.

Figure B.1 is a graphical representation of a process.

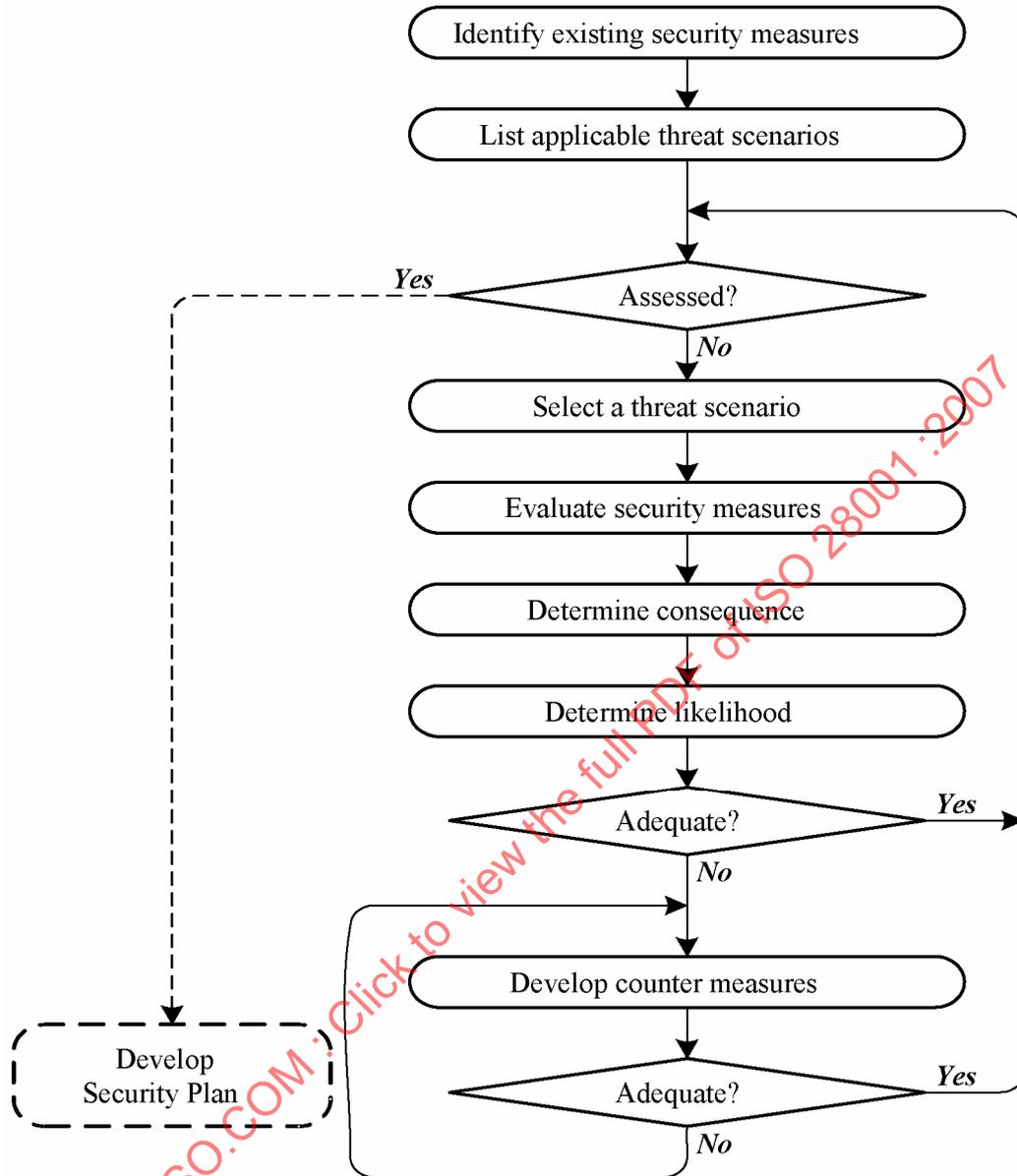


Figure B.1 — Graphical representation of a methodology for security risk assessment

B.2 Step one – Consideration of the security threat scenarios

The security assessment should consider as a minimum the security threat scenarios listed in Table B.1. The security assessment should also consider other scenarios identified by government authorities, supply chain management or the security professional conducting the assessment.

Table B.1 — Security threat scenarios to the supply chain

Example security threat scenarios	Application example
1 Intrude and/or take control of an asset (including conveyances) within the supply chain	Damage/destroy the asset. Damage/destroy outside target using the asset or goods. Cause civil or economic disturbance. Take hostages/kill people.
2 Use the supply chain as a means of smuggling	Illegal weapons into or out of the country/economy. Terrorist into or out of the country/economy.
3 Information tampering	Locally or remotely gaining access to the supply chain's information/documentation systems for the purpose of disrupting operations or facilitating illegal activities.
4 Cargo Integrity	Tampering, sabotage and/or theft for the purpose of terrorism.
5 Unauthorized use	Conducting operations in the international supply chain to facilitate a terrorist incident (e.g. using the means of transport as a weapon).
6 Others	

During the assessment consider the following.

- 1) Access control
 - on premises of the organization in the supply chain, including the neighbourhood;
 - on the means of transportation (truck, rail, air, barge, ship, etc.);
 - on information;
 - others.
- 2) Means of transportation (trucks, railway, barges, aircraft, ships, etc.), taking into account
 - normal operation;
 - maintenance shops (e.g. yards);
 - changes due to e.g. break downs;
 - change of means;
 - conveyances while at rest;
 - using means of transport as a weapon;
 - other.

- 3) Handling:
 - loading;
 - manufacturing;
 - storage (including intermediate storage);
 - transfer;
 - unloading;
 - deconsolidation/consolidation;
 - other.
- 4) Transportation of goods by
 - air;
 - road;
 - rail;
 - inland waterway shipping;
 - ocean shipping;
 - other.
- 5) Intrusion detection/prevention applied to shipments.
- 6) During inspections, e.g. vehicle inspections.
- 7) Employees:
 - level of competence, training and awareness;
 - integrity;
 - other.
- 8) Use of business partners.
- 9) Communication internal/external:
 - information exchange;
 - emergency situations;
 - other.
- 10) Handling or processing of information about cargo or transport routes:
 - data protection;
 - data assurance;
 - other.