INTERNATIONAL STANDARD

ISO 28000

First edition
2007-09-15

Specification for security management systems for the supply chain

Spécifications pour les systèmes de management de la sûreté pour la chaîne d'approvisionnement

Reference number
ISO 28000:2007(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 28000 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 28000 cancels and replaces ISO/PAS 28000:2005, which has been technically revised

Introduction

This International Standard has been developed in response to demand from industry for a security management standard. Its ultimate objective is to improve the security of supply chains. It is a high-level management standard that enables an organization to establish an overall supply chain security management system. It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs. Since supply chains are dynamic in nature, some organizations managing multiple supply chains may look to their service providers to meet related governmental or ISO supply chain security standards as a condition of being included in that supply chain in order to simplify security management as illustrated in Figure 1.

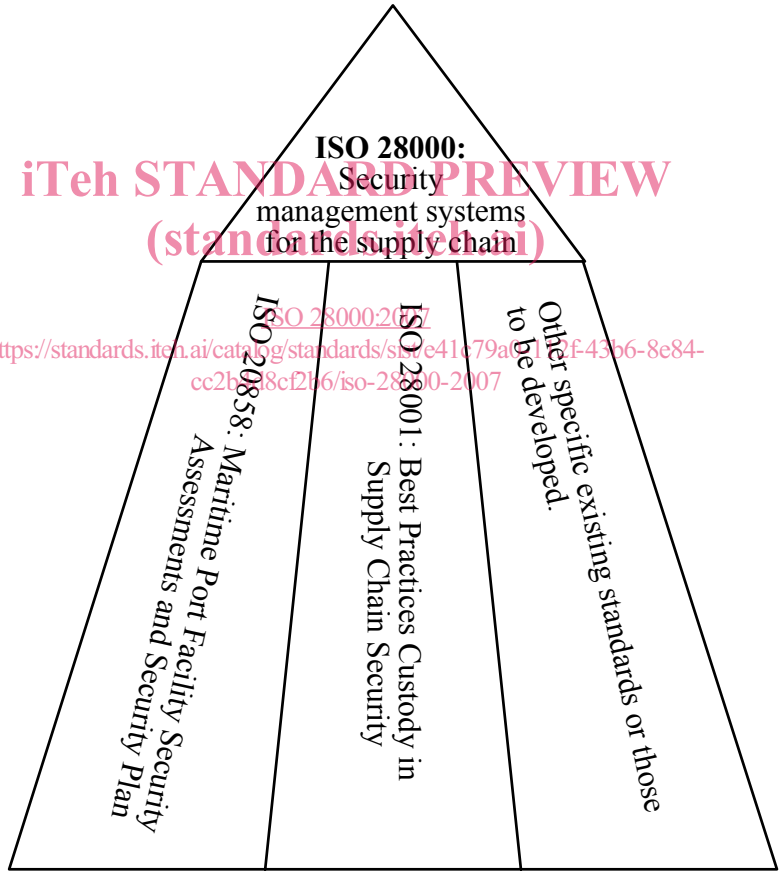

Figure 1 — Relationship between ISO 28000 and other relevant standards

This International Standard is intended to apply in cases where an organization's supply chains are required to be managed in a secure manner. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

Compliance with an International Standard does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system with this International Standard may be verified by an external or internal auditing process.

This International Standard is based on the ISO format adopted by ISO 14001:2004 because of its risk based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2000) may be able to use their existing management system as a foundation for a security management system as prescribed in this International Standard. It is not the intention of this International Standard to duplicate governmental requirements and standards regarding supply chain security management to which the organization has already been certified or verified compliant. Verification may be by an acceptable first, second, or third party organization.

NOTE This International Standard is based on the methodology known as Plan-Do-Check-Act (PDCA). PDCA can be described as follows.

— Plan: establish the objectives and processes necessary to deliver results in accordance with the organization's security policy.

— Do: implement the processes.

— Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.

— Act: take actions to continually improve performance of the security management system.

Specification for security management systems for the supply chain

1 Scope

This International Standard specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

This International Standard is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

a) establish, implement, maintain and improve a security management system;

b) assure conformance with stated security management policy;

c) demonstrate such conformance to others;

d) seek certification/registration of its security management system by an Accredited third party Certification Body; or

e) make a self-determination and self-declaration of conformance with this International Standard.

There are legislative and regulatory codes that address some of the requirements in this International Standard.

It is not the intention of this International Standard to require duplicative demonstration of conformance.

Organizations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.

2 Normative references

No normative references are cited. This clause is included in order to retain clause numbering similar to other management system standards.

3 Terms and definitions

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

3.1
facility
plant, machinery, property, buildings, vehicles, ships, port facilities 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 software code that is critical to the delivery of security and the application of security management.

3.2
security
resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain

3.3
security management
systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts therefrom

3.4
security management objective
specific outcome or achievement required of security in order to meet the security management policy

NOTE It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.

3.5
security management policy
overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements

3.6
security management programmes
means by which a security management objective is achieved

3.7
security management target
specific level of performance required to achieve a security management objective

3.8
stakeholder
person or entity having a vested interest in the organization's performance, success or the impact of its activities

NOTE Examples include customers, shareholders, financiers, insurers, regulators, statutory bodies, employees, contractors, suppliers, labour organizations, or society.

3.9
supply chain
linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport

NOTE The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user.

3.9.1
downstream
refers to the actions, processes and movements of the cargo in the supply chain that occur after the cargo leaves the direct operational control of the organization, including but not limited to insurance, finance, data management, and the packing, storing and transferring of cargo

3.9.2
upstream
refers to the actions, processes and movements of the cargo in the supply chain that occur before the cargo comes under the direct operational control of the organization, including but not limited to insurance, finance, data management, and the packing, storing and transferring of cargo

3.10
top management
person or group of people who directs and controls an organization at the highest level

NOTE Top management, especially in a large multinational organization, may not be personally involved as described in this International Standard; however top management accountability through the chain of command shall be manifest.

3.11
continual improvement
recurring process of enhancing the security management system in order to achieve improvements in overall security performance consistent with the organization's security policy

4 Security management system elements

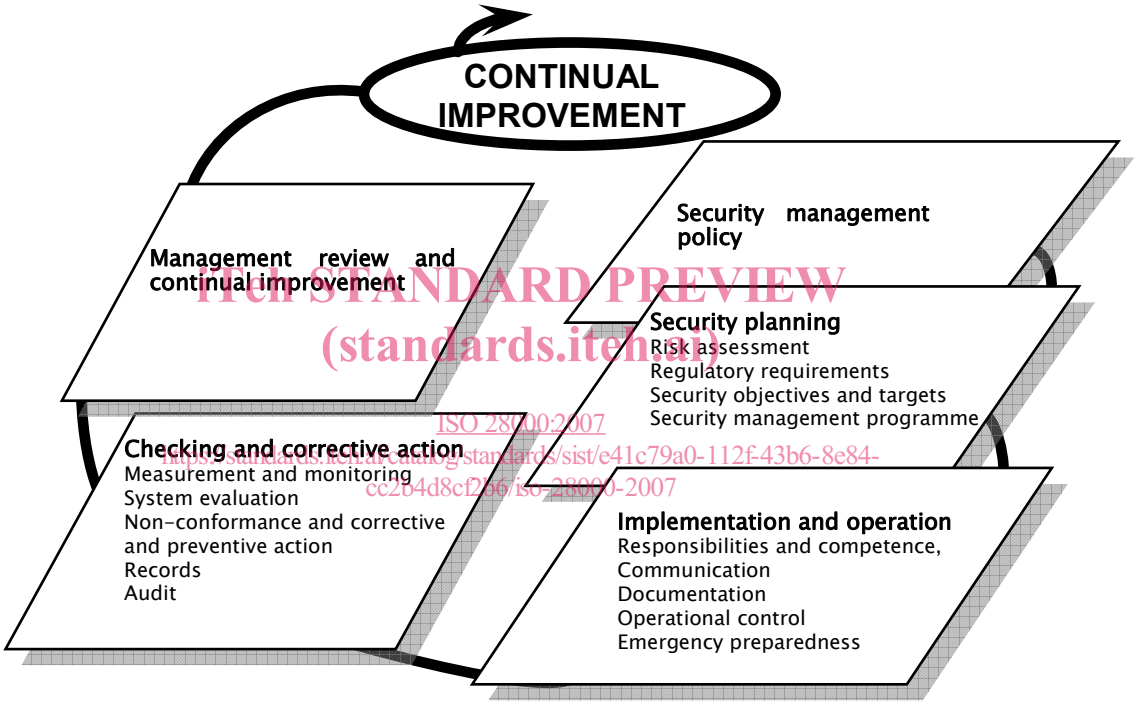

Figure 2 — Security management system elements

4.1 General requirements

The organization shall establish, document, implement, maintain and continually improve an effective security management system for identifying security threats, assessing risks and controlling and mitigating their consequences.

The organization shall continually improve its effectiveness in accordance with the requirements set out in the whole of Clause 4.

The organization shall define the scope of its security management system. Where an organization chooses to outsource any process that affects conformity with these requirements, the organization shall ensure that such processes are controlled. The necessary controls and responsibilities of such outsourced processes shall be identified within the security management system.

4.2 Security management policy

The organization's top management shall authorize an overall security management policy. The policy shall:

a) be consistent with other organizational policies;

b) provide the framework which, enables the specific security management objectives, targets and programmes to be produced;

c) be consistent with the organization's overall security threat and risk management framework;

d) be appropriate to the threats to the organization and the nature and scale of its operations;

e) clearly state the overall/broad security management objectives;

f) include a commitment to continual improvement of the security management process;

g) include a commitment to comply with current applicable legislation, regulatory and statutory requirements and with other requirements to which the organization subscribes;

h) be visibly endorsed by top management;

i) be documented, implemented and maintained;

j) be communicated to all relevant employees and third parties including contractors and visitors with the intent that these persons are made aware of their individual security management-related obligations;

k) be available to stakeholders where appropriate;

l) provide for its review in case of the acquisition of, or merger with other organizations, or other change to the business scope of the organization which may affect the continuity or relevance of the security management system.

NOTE Organizations may choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive the security management system (parts of which may be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to its stakeholders and other interested parties.

4.3 Security risk assessment and planning

4.3.1 Security risk assessment

The organization shall establish and maintain procedures for the ongoing identification and assessment of security threats and security management-related threats and risks, and the identification and implementation of necessary management control measures. Security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the operations. This assessment shall consider the likelihood of an event and all of its consequences which shall include:

a) physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action;

b) operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety;

c) natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective;

d) factors outside of the organization's control, such as failures in externally supplied equipment and services;

e) stakeholder threats and risks such as failure to meet regulatory requirements or damage to reputation or brand;

f) design and installation of security equipment including replacement, maintenance, etc.

g) information and data management and communications;

h) a threat to continuity of operations.

The organization shall ensure that the results of these assessments and the effects of these controls are considered and, where appropriate, provide input into:

a) security management objectives and targets;

b) security management programmes;

c) the determination of requirements for the design, specification and installation;

d) identification of adequate resources including staffing levels;

e) identification of training needs and skills (see 4.4.2);

f) development of operational controls (see 4.4.6);

g) the organization's overall threat and risk management framework.

The organization shall document and keep the above information up to date.

The organization's methodology for threat and risk identification and assessment shall:

a) be defined with respect to its scope, nature and timing to ensure it is proactive rather than reactive;

b) include the collection of information related to security threats and risks;

c) provide for the classification of threats and risks and identification of those that are to be avoided, eliminated or controlled;

d) provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation (see 4.5.1).

4.3.2 Legal, statutory and other security regulatory requirements

The organization shall establish, implement and maintain a procedure

a) to identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks, and

b) to determine how these requirements apply to its security threats and risks.

The organization shall keep this information up-to-date. It shall communicate relevant information on legal and other requirements to its employees and other relevant third parties including contractors.