PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 28004-3

First edition
2012-07-15

Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 —

Part 3:
Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

Systèmes de management de la sûreté pour la chaîne d'approvisionnement — Lignes directrices pour la mise en application de l'ISO 28000 —

Partie 3: Lignes directrices spécifiques supplémentaires concernant la mise en oeuvre de l'ISO 28000 pour l'utilisation dans les petites et moyennes affaires (autres que les ports marins)

Reference number
ISO/PAS 28004-3:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv

Introduction v

1 Scope 1
1.1 Additional guidance 1
1.2 Documentation 14
1.3 Guidance for small and medium sized businesses obtaining advice and certification 14
1.3.1 Demonstrating conformance with ISO 28000 by audit 14
1.3.2 Certification of ISO 28000 by third party certification bodies 15

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/PAS 28004-3 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*.

ISO/PAS 28004 consists of the following parts, under the general title *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000:*

— *Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations*

— *Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)*

— *Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective*

Introduction

"**ISO 28000:2007,** ***Specification for security management systems for the supply chain***", and the guidance contained in ISO 28004, have been developed in response to the need for a recognizable supply chain management system evaluation criteria (validation process) against which their security management systems can be assessed and certified for determining conformance with ISO 28000 and ISO 28004. The guidance currently contained in ISO 28004 is designed to assist organizations adopting ISO 28000. Because the types of organizations that can use ISO 28000 are vast, the guidance provided in ISO 28004 is general in nature. As a result, some smaller organizations have had difficulty in defining the scope of measures needed to address each of the requirements established in ISO 28000. Therefore, the purpose of this part of ISO/PAS 28004 is to provide guidance and amplifying information that can be used by Medium and Small Businesses (other than marine ports) to assist them in defining the scope of validation and verification measures needed to comply with the security provisions specified in ISO 28000 and ISO 28004.

ISO 28000 requires that stakeholder organizations evaluate the capabilities of their security protection management plans and procedures through periodic reviews, testing, post-incident reports, and training exercises to measure the effectiveness of their installed security protection systems and methods. It is critical to the overall continued end-to-end safety of the supply chain that stakeholder organizations ensure the transportation industry that they have sufficient safeguards in place to protect the integrity of the supply chain while those goods are under their direct control. The failure by one of the stakeholder organizations to protect the supply chain from any one of the global threats and operational risks can severely impact the integrity of the system and erode the confidence of those who depend on the secure transportation of their valuable goods.

Medium and small businesses stakeholder organizations are an integral part of the supply transportation system and will be required to conduct these performance capabilities reviews and verify to the transportation industry that they are in conformance with relevant legislation and regulations, industry best practices and conformance with its own security policy and objectives based on the identified threats and risks to their operations. The information contained in this part of ISO/PAS 28004 provides guidance and criteria for evaluating the quality of medium and small businesses (other than marine ports) security management plans developed in accordance with ISO 28000 to protect the integrity of the supply chain. The amplifying information is designed to enhance, but not alter, the general guidance currently specified in ISO 28004. No alterations to ISO 28004, other than the addition of supplements, are made.

Disclaimer

This part of ISO/PAS 28004 does not purport to include all necessary provisions of a contract between supply chain operators, suppliers and stakeholders. Users are responsible for its correct application. Conformance with this part of ISO/PAS 28004 does not of itself confer immunity from legal obligations.

Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 —

Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)

1 Scope

This part of ISO/PAS 28004 has been developed to supplement ISO 28004-1 by providing additional guidance to medium and small businesses (other than marine ports) that wish to adopt ISO 28000. The additional guidance in this part of ISO/PAS 28004, while amplifying the general guidance provided in the main body of ISO 28004-1, does not conflict with the general guidance, nor does it amend ISO 28000.

1.1 Additional guidance

ISO 28000 is designed to be adopted by any size organization interested in better securing their supply chain or services they provide to supply chain operators. The main body of ISO 28004 is designed to provide guidance to organizations of any size that wish to adopt ISO 28000. Because ISO 28004 is designed to provide guidance to a wide size range of organizations it may appear more complex than is needed by a smaller sized organization. The purpose of this part of ISO/PAS 28004 is to simplify the guidance for use by smaller sized organization. Entities using this part of ISO/PAS 28004 for guidance should refer to the main body of ISO 28004 when more information on specific issues is needed than is provided in this part of ISO/PAS 28004. The guidance provided in this part of ISO/PAS 28004 does not amend ISO 28000 or the main body of ISO 28004. Where specific methodologies are discussed in this part of ISO/PAS 28004 they are provided for illustrative purposes (to explain what needs to be accomplished) and other methodologies could be substituted.

Organizations adopting ISO 28000 will need to;

— Specify what their objectives are in regard to providing supply chain security,

— Assess the current state of supply chain security,

— Develop plans that will include existing supply chain processes and procedures, and any additional processes/procedures or systems that have been identified as necessary to meet the stated supply chain security objectives,

— Train personnel as to their duties and responsibilities as defined in the supply chain security plan,

— Install/maintain any systems or equipment specified in the supply chain security plan,

— Begin execution of the supply chain security plan

— Monitor performance of the supply chain security plan execution,

— Periodically reassess the state of supply chain security to detect changes in conditions including new threats,

— Periodically test the organization's plans (exercises) and investigate any supply chain security incidents,

— Update objectives, plans, and personnel training based on input from performance monitoring, reassessments, exercises, or investigations.

Users of ISO 28004 that have not previously worked with management standards will note the use of the words 'Intent', 'Input', and 'Output' that are used in regard to each requirement discussed in this standard. Intent is used as the title of the clause that explains what the organization needs to accomplish. Input is used as the title of the clause that explains what needs to be analyzed or considered. Output is used as the title of the clause that explains what the organization's objectives are or what actions will be taken in regard to that specific requirement.

Step 1 - Preparatory work

Prior to beginning the process of adopting ISO 28000 an organization may wish to consider whether they wish to include all or specific parts of their organization within the supply chain security management system (within the scope of application). The organization is not limited in what it should consider in making this decision, however, it may wish to consider some of the following in making this decision:

— Its corporate objectives

— Customer needs or expectations

— Government interests, if the management system is being adopted to address a government policy or program

— Its familiarity or lack of familiarity with ISO management systems

Within the planned scope of application, the security management system should be extended to all areas and functions related to the supply chain. To help identify what areas and functions may be involved the organization may consider but not be 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.

— Transportation routes and means of conveyance used by the various modes of transportation.

— Other.

Step 2 - Setting 'Security Management Policy' (Clause 4.2 in ISO 28000 and 28004-1)

After the scope of applicability has been preliminarily determined the next step will be establish the Security Management Policy. Security Management Policy is very important since the entire supply chain security management system will be built upon it and if certification is sought, the policy will become the criteria upon which all objectives, activities and plans will be evaluated.

While it may appear that Security Management Policy would be established first and then an assessment of existing conditions would be conducted policy, there is synergy between them as actual initial conditions become known and resource needs are identified.

The security management policy should be contained in a statement that has been endorsed by senior management. The policy must be meaningful and clearly state the overall/broad security management objectives of the organization. To be meaningful they should reflect known security threats and provide a reasonable expectation that the organization will be able to better manage these threats than an organization that has not adopted a proactive management approach. They should also be appropriate to the size and nature of the organization and include a commitment to continual improvement. For illustrative purposes the following policy statement is provided.

BETA TRUCKING LTD - OUR SECURITY POLICY

— Maintain a cargo loss/damage rate at least X% lower than the industry average for the markets served

— Comply with all government transportation/security regulations applicable in markets served

— Meet or exceed the security practices specified by the World Customs Organization for an Authorized Economic Operator (note: this policy might be used if the supply chain moves import or export goods)

— Investigate all loss claims and security incidents and make adjustments

— Continually seek to improve supply chain security and operational efficiency, making changes when feasible

— Cooperate fully with government authorizes if illegal smuggling is detected or suspected

The policy statement should be known to all personnel that could be affected by them including outside parties to the extent needed. If some of the policies need to be kept confidential (for example, cooperating with police or customs when smuggling is detected) the company may restrict their distribution. Organizations may use their policy statements in advertizing.

The policy statement should be documented and kept up-to-date with revisions. When the policy statement is revised all previous editions should be replaced.

Step 3 - Conducting the 'security assessment' (ISO 28000 clause 4.3.1, ISO 28004-1 clause 4.3)

Organizations adopting ISO 28000 are required to conduct a security assessment of the supply chains and their support services that are contained within the scope of application set by management. A security assessment evaluates overall system security by comparing existing security and operational processes and measures against a list of known threat scenarios (risks) to determine if risk is being adequately managed. In general risk is considered to be managed if the likelihood of a medium or high consequence supply chain disruption is limited to a low likelihood situation.

NOTE Care should be taken in managing large complex or multiple supply chains where each is critical to the organization in regard to low likelihood situations. If separate assessments are conducted on each supply chain the true magnitude of the likelihood of a disruption may not be readily apparent.

It is important that all aspects of the security assessment be documented including;

— Personnel involved and their qualifications to conduct the assessment

— Description of the methodology used including a definitions of any terms or numerical/alphabetical characters used in the methodology to describe probability, likelihood, consequence, criticality, or effectiveness

— The threat scenarios that were used during the assessment

— Description of the scope of application

— A listing of existing plans or procedures that were reviewed as part of the assessment

— Assumptions made (if any)

— Sufficient explanations, photographs, diagrams or other descriptors to justify the findings of the assessment

— Aspects of the supply chain that need addition security measures (countermeasures needed)

— Date the assessment was completed

Neither ISO 28000 nor the main body of ISO 28004-1 specify in detail the qualifications required for the personnel conducting the assessment. However, based on the results expected organizations adopting ISO 28000 may wish to use the following general guidance in assembling their assessment team.

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 supply chain contained within the scope of application.

— Applying appropriate measures to avoid unauthorized disclosure of, or access to, security sensitive material.

— Operations and procedures involved in the 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.

— Knowledge of applicable laws, regulations, and legal policies and the government agencies involved.

— Understanding of ISO 28000 and ISO 28004.

Supply chains that are more complex or span numerous operating environments will require more qualified people to conduct assessments than simpler supply chains.

Step 4 - Identification of security threats (threat scenarios)

No security assessment can address all threat scenarios therefore it is important that the assessment team both develop a reasonable list of threat scenarios and document the ones they used during the assessment. In developing a list of threat scenarios the assessment team may wish to obtain input from numerous sources including; corporate records, knowledgeable people within the supply chain, industry associations, insurance companies, and appropriate government authorities. Although not required by ISO 28000, threat scenarios could include accidents and forces of nature. For illustrative purposes, the following list of threat scenarios is provided.

Table 1 — Threat scenarios

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	Moving illegal weapons/goods/currency in the supply chain
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 of the goods or conveyances in the supply chain
5 Intimidation of employees to permit illegal activities	Criminal elements apply pressure to supply chain employees to facilitate illegal activity in the supply chain.

Step 5 - Consequence

After the scope of application and the threat scenarios have been developed and documented the assessment team will need to document expected consequences of each threat scenario. Although there are many methods of defining or classifying consequence the following method is fairly simple and effective for many situations. (Note: other methodologies may be used).

An evaluation of consequences should consider potential loss of life and economic loss. The consequences of each security incident evaluated in the supply chain should be classified as high, medium, or low (see Table B.2). A numerical system may be used in the assessment process, as long as the numerical results are converted to a qualitative system.

Rationales for the classifications of consequences for each security incident should be documented.

Care should be taken in establishing values of “high”, “medium” and “low” consequences. The use of excessively low threshold values may result in the requirement that countermeasures be considered for more security threat scenarios than are needed. However, using excessively high threshold values may omit countermeasures for security threat scenarios involving consequences that the organization or government under which it is operating cannot tolerate.

— A “high” consequence classification may be considered as a consequence that would be unacceptable in all but low likelihood situations.

— A “medium” classification of consequence may be considered as a consequence that would be unacceptable in a high likelihood situation.

— A “low” classification of consequence may be considered as a consequence that is normally acceptable.

Acceptability should not be confused with desirability or approval. Rather, acceptability could be considered as a judgment of the amount of possible damage that the organization or government under which it is operating is willing to accept under certain conditions related to probability. An organization or government may determine that the possibility of a certain level of damage may be undesirable yet acceptable.