BS ISO 28004-3:2014

BSI Standards Publication

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)

National foreword

This British Standard is the UK implementation of ISO 28004-3:2014.

The UK participation in its preparation was entrusted to Technical Committee SME/32, Ships and marine technology - Steering committee.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 77201 6

ICS 47.020.99

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2014.

Amendments issued since publication

Date	Text affected

BS ISO 28004-3:2014

INTERNATIONAL STANDARD

ISO 28004-3

First edition
2014-02-01

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 28004-3:2014(E)

COPYRIGHT PROTECTED DOCUMENT

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 8, *Ships and marine technology*.

This first edition of ISO 28004-3 cancels and replaces ISO/PAS 28004-3:2012.

ISO 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 1: General principles*

— *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 business (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 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 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 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.

INTERNATIONAL STANDARD **ISO 28004-3:2014(E)**

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 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 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.

2 Normative references

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

ISO 28000:2007, *Specification for security management systems for the supply chain*

ISO 28004-1:2007, *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles*

3 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 28004 is to simplify the guidance for use by smaller sized organization. Entities using this part of ISO 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 28004. The guidance provided in this part of ISO 28004 does not amend ISO 28000 or the main body of ISO 28004. Where specific methodologies are discussed in this part of ISO 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 part of ISO 28004. 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 analysed 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 ISO 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 advertising.

— The policy statement should be documented and kept up-to-date with revisions as required in ISO 28000, Clause 4.4.4. 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.

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;

— a 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 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.

Table 2 — Classification of consequence

Assign a rating	Consequence
High	**Death and Injury** - loss of life on a certain scale **and /or** **Economic Impact** - major damage to a asset and/or infrastructure preventing further operations **and /or** **Environmental Impact** - complete destruction of multiple aspects of the eco-system over a large area
Medium	**Death and Injury** - for example loss of life **and /or** **Economic Impact** – for example damage to asset and/or infrastructure requiring repairs **and /or** **Environmental Impact** – for example long term damage to a portion of the eco-system
Low	**Death and Injury** – injuries but no loss of life, **and /or** **Economic Impact** - minimal damage to a asset and/or infrastructure and systems, **and /or** **Environmental Impact** – some environmental damage

Step 6 - Review of existing conditions

After the consequences are defined and documented the assessment team would normally conduct a review of all the supply chain operations, functions, processes (including information systems), plans, and measures in place within the scope of application. This review should be well documented in manner that would allow permit a knowledgeable person, that was not involved in the review, to understand the conclusions reached by the assessment team.

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.
11) External information
   - legal;
   - orders by authorities;

— industry practices;

— accidents and incidents;

— first response capability and response times;

— other.

The use of checklists may be useful. The following performance review list shown in Table 3 may be useful 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 3 — 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			
• Does the organization have in place measures that addresses — 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?			

Table 3 *(continued)*

Factor	Yes	No	Comments
• 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?			
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[1] 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 17712[2] 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?			

Table 3 *(continued)*

Factor	Yes	No	Comments
• If a closed cargo transport unit is used, is it inspected for contamination by the party stuffing immediately before stuffing?			
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: — Front wall — Left side — Right side — Floor — Ceiling/Roof — Inside/outside closure — Outside/Undercarriage			

Step 7 - Evaluation of likelihood

NOTE Likelihood is defined as the ease or difficulty with which a security threat scenario could progress to become a security incident. It is not the probability that a security incident will occur. If the assessment team is assessing the threats posed by forces of nature or accidents the assessment team could also include or substitute probability, drawn from historical records, in assessing those threats.

After or during the review of existing conditions the assessment team will be required to make a determination of likelihood for each threat scenario. If multiple locations are involved the assessment team may wish to consider each location separately. In making this determination the status of physical and operational security measures in the supply chain as documented (possibly using the security performance review list) should be taken into account in classifying potential security incidents. Physical security measures include objects that impede or detect unauthorized access to a target. Operational security measures include people and procedures that impede or detect unauthorized access to a target. The likelihood of each security incident occurring at a particular asset should be classified as high, medium and low.

— **High likelihood** should be used when the security measures in place offer little resistance to the security incident occurring. If a numerical system is used in the assessment process, the numerical results should be converted into this qualitative system.

— **Medium likelihood** should be used when the security measures in place offer moderate resistance to the security incident occurring.

— **Low likelihood** should be used in cases where the security measures in place offer substantial resistance to the security incident occurring.

The rationale for the classification of likelihood assigned to each security incident should be documented.

Step 8 - Threat scenario scoring

Drawing upon the list of threat scenarios, the consequences assigned to them and the likelihood of each the assessment team should determine if additional measures are needed to manage the risk from any of the threat scenarios. One method of making this determination is the use of a threat scoring chart, Table 4 is an example of such a chart and could be used to determine when countermeasures should be considered for specific security incidents.

Table 4 — Threat scoring chart

		Likelihood classification		
		High	**Medium**	**Low**
Consequence classification	**High**	**Countermeasures**	**Countermeasures**	**Consider***
	Medium	**Countermeasures**	**Countermeasure or Consider as appropriate**	**Document**
	Low	**Consider**	**Document**	**Document**

Identification of countermeasures is required for threat scenarios that score high in both likelihood and consequences, as well as for those scoring at medium likelihood and high consequences. Other threat scenarios need not include countermeasures, unless they are considered advisable by the evaluator. The person assessing the security should list each threat scenarios required to be considered for countermeasures.

Step 9 - Development of countermeasures

If the development of a countermeasure is required or considered advisable by the evaluator both the consequences and/or likelihood of the security threat scenario should be considered for mitigation. Reducing the likelihood of the security threat scenario succeeding or reducing the harm that can be caused by the security threat scenarios to a level in which additional countermeasures are no longer required is the objective.

Countermeasures may come under the following actions.

— **Treat:** may be organizational and/or physical measures.

— **Transfer:** transfer of the risk may be subcontracting, physical transfer to other locations, time, etc.

— **Terminate:** it is possible that due to the level of risk the organization decides not to continue the activities.

In certain circumstances an organization may have to tolerate (see below) a risk due to impracticality of the countermeasures needed, lack of authority to impose the countermeasures needed or other insurmountable factors.

Tolerate the situation is such that no action can be taken by the organization. These activities and evaluations should be documented and under periodic review.

Step 10 - Implementation of countermeasures

New countermeasures represent a change to operational practices and need to be enacted in accordance with the organization's management system to ensure that adequate resources are available; the impact on other operations is managed and the change has the support of management.

Step 11 - Evaluation of countermeasures

Using the methods specified in this part of ISO 28004, each countermeasure should be assessed for effectiveness in lowering the likelihood or consequences (or a combination of them) until the security risk no longer requires that additional countermeasures be considered. The countermeasure achieving this is considered to be effective, and should be documented in the security assessment report.

Step 12 - Repetition of the process

After countermeasures have been developed and evaluated as effective continue the process for the next security threat scenario until the scenario list is depleted.

Step 13 - Continuation of the process

The process of assessment is continual, security must be monitored continually to ensure security measures are performing as intended and the assessment process should be performed as needed.

Step 14 - Development of the security plan

How the management systems works, the roles and responsibilities of all involved and additional aspects discussed below need to be documented. Documentation would be contained in organizational operating plans, in separate documents, and/or as annexes to other organizational documents. To simplify this discuss this body of documentation will be called the security plan. The security plan should include, but should not be limited to, descriptions of the following.

— The portion of the supply chain that is covered by the plan.

— The security-related duties of all security personnel.

— The security management structure including the name of the person designated as manager of security and the role of top management.

— 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.

— How the supply chain security management system will be monitored.

The Security Plan should contain procedures including but not limited to the arrangements that do the following.

— All the processes and measures that the assessment team reviewed and determined were applicable to supply chain security and the addition countermeasures determined necessary as a result of the supply chain assessment. These may include:

  — 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.

4 Documentation

The organization should maintain the current 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 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.

— Results on management system monitoring and changes that have been made.

5 Guidance for small and medium-sized businesses obtaining advice and certification

5.1 General

Organizations intending to implement ISO 28000 are not obliged to obtain the services of an outside consultant. If an organization determines that it needs advice or help with carrying out security assessments, developing security plans, or implementing the necessary requirements, it may seek external consulting services. It is, however, the responsibility of the organization seeking advice to check and verify the competence of consultants offering advisory services, for example by seeking recommendations, following up references or by reviewing work carried out. Consultants that provide services to the organization would be precluded from participating in third party audits of the same organization.

5.2 Demonstrating conformance with ISO 28000 by audit

ISO 28000 is a requirements specification intended to help organizations, which opt to voluntarily implement the requirements, establish and demonstrate an appropriate level of security within those part(s) of the international supply chain(s) they control. It therefore serves as a basis for determining, validating or demonstrating the level of existing security within organizations' supply chain(s) through a first, second or third party audit process, or by any government agency that choose to use compliance with this part of ISO 28004 as the basis for acceptance into their supply chain security programmes.

Types of audit:

— A first party audit is the self determination of conformance by the organization itself.

— A second party audit is the determination or verification of an organization's conformance to agreed criteria by another organization, agency or body which has a vested interest in the organization's operations in the supply chain.

— A third party audit is a determination or verification of conformance to agreed criteria by an organization independent of all parties.

5.3 Certification of ISO 28000 by third party certification bodies

If demonstration of compliance is sought through the third party audit process then the organization seeking certification should consider selecting a third party certification body accredited by a competent accreditation body that complies with internationally recognized rules, codes of practice and audit protocols, such as ISO/IEC 17021 and ISO 19011.

Bibliography

[1] ISO/IEC 17021, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[2] ISO 17712, *Freight containers — Mechanical seals*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] WCO (2012), SAFE framework of standards to secure and facilitate global trade

ICS 47.020.99
Price based on 15 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™