INTERNATIONAL STANDARD

ISO 28004-2

First edition
2014-02-01

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

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

Partie 2: Lignes directrices pour l'adoption de l'ISO 28000 lors de l'utilisation dans les opérations portuaires petites et moyennes

Reference number
ISO 28004-2:2014(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.

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 28004-2 cancels and replaces ISO/PAS 28004-2:2012. It also incorporates the Amendment ISO 28004-1:2007/DAmd1.

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 businesses (other than marine ports)*

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

Introduction

This part of ISO 28004 is designed to provide guidance and amplifying information for medium and small seaports desiring to adopt ISO 28000. 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, will be undertaken.

Relationship with ISO relevant technical standards

There are several established and pending related ISO technical standards that when coupled with this part of ISO 28004, provide additional guidance and instructions for the seaport operators for establishing their security management plans and evaluating the capability of those plans to protect the integrity of the supply chain cargo while under their direct control. These international standards: ISO 20858, ISO 28001, ISO 28002, ISO 28003, including the ISO 28004 series are referenced in this part of ISO 28004 and in order to provide specific guidance steps to operators. The relevance of these international standards to ISO 28000 is presented in Table 1.

Table 1 — Relevant ISO technical standards

ISO technical standard	Technical description
ISO 28004-1	Provides guidance to certifying bodies on assessing conformance of an organization with the requirements of ISO 28000
ISO 20858	Provides a professional interpretation of the IMO ISPS for port facility security and guidance for evaluating the port security management plans and installed operational procedures.
ISO 28001	Provides security requirements addresses the core security requirements of the World Customs Organization (WCO) Authorized Economic Operator Program
ISO 28002	Provides guidance on establishing a policy to enhance the resilience of an organization's supply chain
ISO 28003	Provides guidance to certifying bodies on assessing conformance of an organization with the requirements of ISO 28000

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

1 Scope

This part of ISO 28004 identifies supply chain risk and threat scenarios, procedures for conducting risks/threat assessments, and evaluation criteria for measuring conformance and effectiveness of the documented security plans in accordance with ISO 28000 and the ISO 28004 series implementation guidelines. An output of this effort will be a level of confidence rating system based on the quality of the security management plans and procedures implemented by the seaport to safeguard the security and ensure continuity of operations of the supply chain cargo being processed by the seaport. The rating system will be used as a means of identifying a measurable level of confidence (on a scale of 1 to 5) that the seaport security operations are in conformance with ISO 28000 for protecting the integrity of the supply chain.

2 Overview

2.1 Objective

The objective of this part of ISO 28004 is to provide guidance to medium and small ports that wish to adopt ISO 28000. This guidance provides a self-evaluation criterion that could be used by these ports as they implement ISO 28000. While the self-certification criteria will not result in a third party certification, it can be used to determine the capability of the seaport stakeholders' security management plans for safeguarding the integrity of supply chain in accordance with the security provisions and guidelines specified in ISO 28000 and the ISO 28004 series. The goal is to develop a risk assessment evaluation rating scale metric that can be used to evaluate the capability of the port security management plans to provide uninterrupted security protection and continuous operations for the supply chain cargo being received, stored, and transferred by the seaport. The use of these self-evaluation criteria will enable the user to determine if the seaport has addressed each requirement of ISO 28000 in adequate detail.

2.2 Background

The International Ship and Port Facility Security (ISPS) Code requires that each maritime port facility develop a comprehensive port facility security plan that includes the cargo under their direct control. The port security plan should address those applications, security systems and operations measures designed to protect the personnel, port facilities, ships at berth, cargo, and cargo transport units, including rail and ground within the port facility physical boundaries from the risks of a security incident (ISO 20858 provides clear guidance on meeting these requirements). ISO 28000 and the ISO 28004 series have established guidelines for protecting the Global Supply Chain at a very high level, but do not provide enough specific detail that would allow a consistent level of implementation to cover all of the security provisions and applications for large, medium and smaller seaports that are integral parts of the global supply chain security infrastructure. To ensure long term and consistent security of the supply chain, there is a need for each of the stakeholders in this integrated global network to be measured and held accountable for contributing to the safety and uninterrupted delivery of goods.

The Medium and Small seaports are an integral part of the supply chain delivery infrastructure especially considering that these ports are typically the first entry points for a majority of the goods

being shipped and distributed to local and international destinations. These smaller ports are the feeder ports for goods being shipped to the larger mega ports for consolidating cargo for distribution to long haul shipment to other mega ports and global destinations. Therefore, it is critical that these Medium and Small sized seaports implement and maintain proven security provisions that can ensure the protection and continued safe passage of goods being shipped through their port facilities.

While ISO 28000 and the ISO 28004 series provide general overviews of the expected requirements to secure the supply chain, there are limited instructions, measurable requirements and acceptance criteria that would allow an entity to create and implement a security management plan that would ensure that the established standards in ISO 28000 were met. Therefore, this part of ISO 28004 is designed to provide the methods, procedures, guidelines and acceptance criteria that will be used for measuring the level of conformance with ISO 28004 security provisions.

2.3 ISO 28000, 4.3.1 requirements for security risk assessment

ISO 28000, 4.3.3 states "When establishing and reviewing its objectives, an organization shall take into account: a) legal, statutory and other security regulatory requirements" The ISPS Code as adopted by each member state establishes such security risk assessment requirements. Clause 4.3.1 of ISO 28000 therefore requires, the seaport stakeholders and governing organization establish and maintain procedures for the ongoing identification and assessment of security threats, security management-related threats and risks, and the identification and implementation of the necessary management control measures to safeguard the supply chain. The security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the seaport operations. This assessment shall consider the likelihood of an event and all of its consequences to the seaport stakeholders, threats to continuity of operations, supply chain security, and disaster recovery. Specifically, the risk assessment should address at a minimum the following:

a) Operational threats and risks, including the control of the security, human factors and other activities, which affect the organizations performance, condition or safety.

b) Natural environmental events (storms, floods, high winds, etc.), which may render security measures and equipment ineffective.

c) Factors outside of the organization's control, such as failures in externally supplied equipment and services, changes in local and international security policies and regulations, and political changes affecting seaport ownership and operations.

d) Stakeholder threats and risks such as failure to meet regulatory requirements, financial constraints, or ownership changes that affect port operations and supply chain security.

e) Design, installation, validation and maintenance of security equipment including installation of new systems and training of staff to operate, repair and maintain.

f) Failure of critical information, data management and communication systems used to manage and safeguard the supply chain.

The seaport stakeholder organizations responsible for providing security protection for supply chain goods shall ensure that the results of these assessments and the appropriate security controls are in place to safeguard the integrity of the supply chain. The seaport Security Management Plan must provide provisions and procedures for addressing the security system objectives, operational requirements, risk assessment and mitigation, continuity of operations and disaster recovery steps. Specifically, the plan should address the following:

— The determination of requirements for the design, specification, installation, certification and operation of security devices and systems;

— Identification of security staffing resources, skill levels, and training needed to operate and maintain security devices and systems (ISO 28000, 4.4.2);

— Identification of the organization's overall threat and risk assessment and management framework to mitigate identified risks.

— Continuity of operation provisions and disaster recovery steps that will be implemented to restore security systems for protecting the supply chain and restore the seaport to full operational status.

The organization shall document and keep the above information up to date and have personnel trained in the understanding and application of the security and operational plans and procedures specified in the plan. The organization's methodology for threat and risk identification, assessment and mitigation shall at a minimum do the following:

— Be clearly defined with respect to its scope, stakeholder roles and responsibilities, expected nature and timing of risks and threats to ensure it is proactive rather than reactive.

— Identify and the monitor the collection of information sources to document existing and determine future supply chain related security threats and risks.

— Provide for the classification of threats and risks and the identification of mitigation steps for those that must be either avoided, eliminated or controlled.

— Provide for the monitoring of actions to ensure effectiveness and the timeliness of their implementation (ISO 28000, 4.5.1) to ensure uninterrupted protection of the supply chain.

The seaport security management plan should be a planned part of the continuous improvement procedures for keeping the seaport personnel and systems current with identified threats, risks and operational security needs required to safeguard the supply chain.

The security threat identification, risk assessment and risk management processes and their outputs should be the basis for developing and implementing a comprehensive supply chain security system. It is important that the links between the security threat identification, risk assessment and risk management processes and the other elements of the security management system are clearly established, continually monitored and updated to reflect any changes in the threats and risks assessments to port operations for safeguarding the supply chain.

2.4 Risk assessment requirements

2.4.1 General

Security threat identification, risk assessment and risk mitigation processes are key tools in the management, control and elimination of risks to the security and continuous operation of the supply chain. The seaport security management plan must address each of these areas and provide specific roles and responsibilities for each stakeholder involved in safeguarding the supply chain.

2.4.2 Medium - small seaport risk assessment considerations

The goal of the document is to create a process for assessing the risk to the Supply Chain and what steps are in place to minimize and prevent major disruptions to the supply chain cargo being transported through the mid and small sized seaports. These seaports are usually the initial entry point for a large segment of the goods being shipped to the larger and mega international seaports. Cargo entering the ports from upstream locations via rail, truck and transport vessels that either transfer or collect cargo stored at the port locations. Therefore the goal is to determine and assess the ability of the port operations to safeguard the cargo and maintain the expected delivery pace of the products as goods past through the seaport.

The inbound collection, processing, storage, loading/unloading of cargo and final outbound shipping requirements and port operations plan and security plans that is designed to have a functional Continuity of Operations Plan (COOP) designed around the identified and perceived risks associated with the amount, flow and type of cargo being handled by the port. For each identified risk and/or threat to the flow of goods through the port must have a plan in place to either avoid, prevent or minimize the impact of the risks with work a rounds and formal disaster recover plans to provide COOP for the

port and the flow of goods. These plans that are developed and maintained by the port operations and associated stakeholders will be evaluated and assigned a certification/level of confidence number that can be used to measure the level of conformance with the ISO 28000 and the ISO 28004 series guidelines for protection of the supply chain.

The major output of the document will be a set of guidelines to assess the conformance of the seaport security management plans with the ISO 28004 series. The guidelines will cover the identification of risks and threats to the seaport operations and the documented procedures and practices implemented by the seaport stakeholders to prevent, detect, respond and restore the port to normal operational status to safeguard and ensure the continuity of operations for the supply chain.

2.4.3 Intent

The intent is to create and document a set of procedures for measuring the capability of the Medium and Small sized seaports to comply with the supply chain security requirements specified in ISO 28000 and ISO 28004 for the identified threats and risks to their seaport operations. Security threat identification, risk assessment and risk management processes are key tools in the management and reduction of security risks to supply chain operations. Security threats and risks can vary greatly across the supply chain infrastructure from minor incidents to full-scale breaches in cargo security. The goal is to (a), identify and characterize those threats and risks that are specific to the smaller seaports; determine the possible impacts to port security operations; (b), evaluate the seaport mitigation processes and prevention steps developed in response to those threats/risks; (c), and then assess the capability of the seaport to maintain the integrity of the supply chain for goods being transported through its facilities. The seaport security management plan will then be evaluated to determine the capability of the seaport to protect the supply chain against the identified threats and risks to their operations.

2.4.4 The process

Security threat identification, risk assessment and risk management processes are key tools in the management of risk. Security threat identification, risk assessment and risk management processes vary greatly across industries, ranging from simple assessments to complex quantitative analyses with extensive documentation. Therefore, the seaport Stakeholder organizations and agencies must maintain a comprehensive security management plan that addresses those threats and risks to their operations.

The seaport stakeholder organizations and agencies responsible for supply chain security, as well as port operations, are required to create and maintain a security management plan that identifies all credible threats and risks to port and security operations and creates mitigation strategies and recovery procedures for safeguarding the integrity of the supply chain. Each seaport operation will be evaluated on quality and capability of their implemented security plan to fully protect the supply chain against the identified threats and risks that it either controls or has influence over. The performance indicators that would be used to measure the capability of the seaport security protection provisions will include at a minimum the following to determine if:

— The ISO security policy and security objectives are being achieved.

— All Identified threats and risks to supply chain security are being controlled and/or mitigated, as appropriate and countermeasures have been implemented and are effective.

— Security personnel are knowledgeable and trained in the security protection, detection, mitigation and recovery procedures needed to safeguard the supply chain.

— Incident recovery and continuity of operations plans (COOP) are well established with adequate provisions for quickly restoring port security equipment and systems designed to protect the supply chain.

— Continuous improvement processes are in place to learn from any security management system failures, including security incidents and near misses.

— Regularity scheduled security training and exercises are being conducted to ensure that stakeholder personnel are current and aware of their assigned roles and responsibilities for protecting and responding to security incidents.

Performance measures for the management of threats and risks to the supply chain will consider the probability of occurrence, vulnerability of the security systems, expected impact to port security operations and recovery steps to ensure continuity of security protection. The performance assessment measures will reflect the capability of the plan for eliminating or reducing to a practicable minimum security risk, either by reducing the likelihood of occurrence or the potential severity of impacts from security related incidents.

2.4.5 Expected inputs

For the medium to small seaport operations, there are at least nine universal risk and threat category areas that have the potential for major disruptions to the supply chain for cargo being transferred in, processed, stored and transferred out by the seaport stakeholder organizations responsible for safeguarding the integrity of the cargo while in port. These categories include the following:

— Accidents that occur in the port facilities involving staff, equipment, cargo and fluid spills.

— Criminal Activities such as theft, vandalism, and contra band smuggling.

— Fire to building facilities, equipment, on board vessels and surrounding port areas.

— Financial issues with port operations and transportation stakeholders.

— Labour unrest including labour strikes, staff shortages and skills trainings

— Mechanical/Equipment breakdowns that put major support items (Cranes, communications equipment, cargo movement loaders) out of commission for extended periods of time.

— Political unrest that includes government restrictions, new policies and regulations that impact port operations.

— Terrorist activities that physically attack/damage port operations and/or disrupt the flow of cargo due to the discovery of contraband that forces the port to close until contraband can be removed and the port cleared for resume normal operations.

— Weather related issues such as natural environmental events (severe storms, wind, heat, cold, ice, snow and floods) that can disrupt operations and render security measures and equipment ineffective for several hours to several days/weeks.

Each of these nine areas represents a level of risk to continuous operations at the seaport that can affect the security of the supply chain. Once the input parameters that describe the nature and level of risk to seaport operations for each of these threat and risk areas are identified, then these inputs become the basis for developing prevention and mitigations strategies to minimize their occurrence and formulate recovery plans when they do occur. For each of the identified areas, a risk assessment, mitigation strategies, and disaster recovery guidelines are discussed in the following clauses.

2.4.6 Expected output

The purpose of this guideline is to establish principles by which the organization can determine whether or not given security threat identification, risk assessment and risk management processes are suitable and sufficient to safeguard the integrity of the supply chain. The certification process will allow seaport operators and supply chain stakeholders to assess the probability that their goods and operations will be secured and processed in a timely matter in accordance with the required security protection policies and procedures and delivery schedules agreed to by the transportation stakeholders and their end user recipient customers. The seaport security management plan documenting the implemented security provisions will be evaluated and assigned of a level of confidence number indicating the assessed quality and capability of the management plan to safeguard the integrity of the supply chain.

2.4.7 Certification process

To ensure consistency and completion of a creditable evaluation process, the certification process should be conducted by a qualified independent organization. The process itself will be comprised of a list of evaluation points and criteria covering the supply chain security threats and risk areas identified in the seaport security management plan. The goal is to have fully trained personnel and/or experienced independent organizations with the required technical expertise, to assess and evaluate the established security plans. ISO 20858 provides specific guidance for specifying the competence and technical expertise required of personnel to conduct a marine port facility security assessment in accordance with ISO 28000 requirements. In addition, ISO 20858 provides specific documentation guidance and requirements for assessing and recording the quality of the port security management plans. Evaluation and certification by an independent qualified third party is envisioned to do the following:

— Validate to the user community that the seaport meets the intended objectives and standards specified in ISO 28000 and the ISO 28004 series for safeguarding the integrity of the supply chain.

— Establish a repeatable process that can be used as a standardized basis for measuring and comparing seaport security plans to an industry standard.

The evaluation will be based on their ability to meet the certification criteria in accordance with the identified risks; mitigation procedures; and, recovery plans associated with the level of seaport operations, traffic flow, cargo type, geographical location, and stakeholder security systems and operational structure for securing the supply chain. An outcome of the evaluation process will be the assignment of assessment quality number that identifies to what level of confidence (1 to 5, with 5 being the highest) that the seaport security management plan will be able to safeguard the supply against the identified risks and threats to seaport operations.

3 Supply chain seaport risk areas

3.1 General

The nine maritime seaport risk areas are discussed in the following paragraphs, including the identification of the types of related risk issues, their risk assessment considerations, mitigation steps to minimize the risks, and recovery guidelines to restoring security protections systems and port operations to their normal operating status. Depending on the operational tempo, stakeholder organizational structure, flow of goods through the seaport, geographical location, government and political considerations, each seaport will have varying levels of threats and risks to their seaport operations in providing security and uninterrupted transportation services to the supply chain. Those that apply for each seaport should be addressed in their security management plan and updated if new threats, risks and/or changes in the operational status of the seaport.

3.2 Accidents — Port operations

3.2.1 Nature of risk

Accidents can be purely random in nature and/or can be categorized as accidents waiting to happen that could have been prevented with better management oversight, staff training and operational procedures. The security of the supply chain will rely on the constant surveillance and protection of cargo while in port by security personnel and security protection systems and equipment. Any accident that disrupts the oversight and protection of cargo must be addressed with specific plans in place to minimize occurrences, prevent where ever possible and execute recovery steps to restore the security coverage to the supply chain. The heavy machinery, loading cranes, cargo movement vehicles, rail and truck off loading devices all pose safety issues for seaport personnel operating those systems and overseeing the security of the supply chain cargo while in port. Industrial accidents involving personnel, equipment, cargo and/or fluid/chemical spills have the potential of comprising the integrity of the supply chain if security provisions and seaport operations are disrupted for any sufficient amount of time.

3.2.2 Risk assessment

The probability of occurrence and severity of the identified risks to operations will need to be assessed. Depending on the nature of the accident, the probability of occurrence and expected impact on security and continuity of operations will need to be determined. The assessment should address the specific impacts to security (lost of key, monitoring and protection systems) and expected vulnerabilities if there is break in security protection. All occurrences, even those that have limited impact on security and port operations should be assessed. Each occurrence must be assessed to determine the level of risk to the supply chain based on the capability of the seaport operators to quickly restore and verify that security systems are operational and that the integrity of the supply chain was not comprised. Any incident assessed as high risk to the supply chain security operations must identify the specific vulnerabilities that could be exposed by the occurrence.

Accidents that involve key security personnel must be identified with immediate provisions made for staff replacements that are trained to perform the required roles and responsibilities. The security plan must address these vulnerabilities and create mitigation steps to avoid, if possible, and if not, planned recovery steps to ensure continued protection of the supply chain.

3.2.3 Mitigation strategies

The port operators and stakeholders need to identify the types of accidents that have occurred at the ports and quantify their specific impacts to port operations. Industrial accidents involving staff, equipment, cargo and fluid/chemical spills can be quantified with historical data showing the frequency, severity of impact to operations and what preventive steps have been taken to minimize the reoccurrence. Preventive safety measures should be put in place that alert and remind the staff of the safety concerns and procedures for avoidance.

The management plan should address the specific processes that will need to be implemented to prevent and restore the system to operational status after each occurrence. The mitigation plans should be in sufficient detail to provide for specific steps by the stakeholders to safeguard the supply chain and restore the seaport to its operational status depending on the nature and expected impact for each of the assessed risks.

3.2.4 Recovery guidelines

The security management plan should provide specific steps that can be measured and assessed to determine the ability of the seaport to safeguard the supply chain and resume normal operations. Accidents that affect key security personnel and/or security equipment and operational systems must have documented recovery procedures that identify specific steps for replacing security staff, equipment and systems. Back up and/or replacement staff must be trained in all aspects of supply chain security including physical protection, inspection and detection procedures, and use of security devices and automated systems. Accidents that shut down port operations need to address procedures that will be followed to safeguard cargo that is in transit or stored at the port until normal port operations are restored.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

3.3 Criminal activity risks

3.3.1 Nature of risk

Criminal activity at the seaport and activities associated with the shipping and arrival of goods being shipped to the seaport or from cargo from upstream sources can bring an immediate halt to all traffic at the seaport. Criminal activities may require the shutting down and or isolation of operational support areas until they can be investigated by law enforcement agencies. In addition, theft of critical equipment items and components may impact operations until replacement items are acquired and put in service.

Depending upon the nature and severity of the issue, delays could be measured in days if port operations have to be truncated. If criminal activities involve port staff then special provisions will have to be addressed by the port operator stakeholders to restore the integrity of the port operations and regain any lost trust with the supply chain community.

3.3.2 Risk assessment

Criminal attractively by definition is covert and difficult to detect and takes on many forms from basic theft of goods and services, smuggling of contra band (drugs, weapons, people, goods), to bribery and fraud. All of these activities are aimed at breaching the security and integrity of the supply chain. Loss of goods, transporting of contra band, fraud and bribery of personnel employed to safe guard the port security operations have the potential for comprising the integrity of the supply chain and damaging the reputation of the seaport and stakeholders. The probability of occurrence and severity of the identified risks to operations will need to be assessed. Depending on the nature of the criminal activity, the probability of occurrence and expected impact on continuity of operations will need to be determined. All occurrences, even those that have limited impact on port security operations should be assessed. If the activities involve the replacement of critical security protection equipment and/or critical personnel, then the assessment must include the availability and procurement of the item and its installation and testing, and the availability of qualified and trained staff, if required, to restore the systems back to full operational status.

Smuggling of contra band goods will present a special set of circumstances when they are discovered/detected by port security personnel. The discovery of illegal drugs, weapons, dangerous materials and/or people will require law enforcement intervention, seizure, and storage of the contra band cargo. Each event has the potential for stopping the flow of cargo and the security management plan must take into account the disruption that these activities will have on the continuity of operations and if security procedures did to be adjusted or enhance to prevent future incidents.

The criminal theft or hacking of computers and computer files will have to be specifically addressed and an assessment made on the impact and time involved to restore the lost data. The management plan should have special provisions for protecting critical data files, including port security plans, that if lost or compromised, would put the supply chain and port operations at risk.

3.3.3 Mitigation strategies

Upon detection of criminal activity, the plan must identify specific steps for that will be followed by each stakeholder organization and agency for stopping, apprehending and assessing the damage/loss experienced by the supply chain cargo. The mitigation plans should be in sufficient detail to provide for specific steps by the stakeholders to safeguard the supply chain and restore the seaport to its operational status depending on the nature and expected impact for each of the assessed risks.

The detection, prevention and apprehension of criminals will required the coordination between local law enforcement agencies and the port stakeholders' responsible for providing security protection for seaport operations. The management plan should address the specific processes and procedures for monitoring, detecting, investigating, and preventing the types of identified criminal risks areas based on historical and intelligence data gathered from local and global law enforcement agencies. Establishing plans for periodic and random inspections of cargo along with automated scanning and detection equipment will help in the discovery of contraband cargo and deter future criminal activities.

Theft of goods entering and stored at the port can be minimized limiting access to the port and requiring security checks, inspections and positive identification of all personnel and vehicles entering/existing the port. The plan should address active and passive monitoring equipment (cameras, security guards, access cards/readers) that can be used to secure the supply chain cargo on a 24/7 basis.

If criminal activities are determined to be from identifiable upstream sources, then additional security inspections should be aimed at those sources and/or restrictions put on of cargo from those identified shipping sources. Suspect shipping sources should require additional inspections and provisions made with law enforcement agencies to assist in the identification, inspection, and seizure of contraband cargo and those involved in the criminal activity.

To control and reduce the risk of seaport personnel involvement, the plan should have detailed hiring and personnel review procedures for background checks, periodic reviews and ethics training for all staff. The management should also have security procedures in place to limit access to seaport facilities using security checkpoints requiring positive identification for all staff and visitors entering the facilities.

3.3.4 Recovery guidelines

The security management plan should provide specific steps that can be measured and assessed to determine the ability of the seaport to safeguard the supply chain and resume normal operations. The roles and responsibilities for each stakeholder should be clearly stated with specific response steps in response to each identified criminal activity. For each actual occurrence, the seaport security detection and prevention processes should be evaluated to determine how well the implemented systems/procedures were able to detect and respond to criminal activity. If vulnerabilities are discovered in the after action reports, then corrections should be make eliminate any identified deficiencies in the supply chain security protection plan.

If systems and/or procedures are found to be deficient, then systems upgrades and security procedures should be enhanced to reduce or eliminate the possibility of future occurrences. For those cases where seaport personnel were complicit in the criminal activity, then hiring and personnel screening procedures will be need improved and policies enacted to provide additional supervision to prevent future occurrences.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

3.4 Fire risks

3.4.1 Nature of risk

Fire at the seaport has the potential for causing major disruptions if it destroys critical buildings, security systems, major equipment, transportation equipment and stored cargo. In addition, fires aboard vessels docked at the port as well as fires in surrounding areas have the potential for causing delays to the delivery of goods to the seaport. The effect of a major fire at a seaport has the potential to shut down the facilities for an extended period of time especially if security and cargo handling systems are out of commission. Damage to critical physical and automated security protection systems (fences, guard booths, camera systems, computer and systems, communications systems) will require the restoration of those systems to operational status before normal seaport operations can resume. The security management plan must address potential fire risk areas and have COOP and disaster recovery plans and procedures in place in order to safeguard supply chain cargo while in port. Special emphasis must be taken to ensure that none of the critical security systems have been compromised by any fire damage as well as safeguarding the cargo from possible tampering by outside agencies responding to the fire.

Fire prevention and mitigation strategies, including the fire fighting capabilities of the seaport to extinguish fires quickly, and the disaster recovery plans will determine the affect on seaport security and cargo handling capabilities of the port stakeholders. The seaport security management plans will be evaluated to determine if the preventive measures, personnel training, and recovery steps are sufficient and effectiveness in safeguarding the integrity of the supply chain for cargo under the seaport's direct control during a fire incident.

3.4.2 Risk assessment

The probability of occurrence and severity of the identified risks to operations will need to be assessed. Depending on the nature of the fire and how much damage was done to the operational capabilities of the seaport, the expected impact on continuity of operations will need to be determined. The assessment should address the expected delay time and the required recovery procedures to return port operations to their normal operational status. All fire incidents, even those that have limited impact on port operations, should be assessed. If the incidents involve the rebuilding of facilities and/or

replacement of critical security protection support equipment, then the assessment must include the availability and procurement of the item, installation and testing, if required, to restore the systems back to full operational status. The lost of computers and computer files that support the command, control and communications between local, regional and international security agencies will have to be specifically addressed and an assessment made on the impact and time involved to restore this data and communications access.

The estimated amount of delay caused by each occurrence will need to be determined in terms of hours, days and weeks. The expected incident delay will be a major factor for establishing the mitigation strategies and recovery procedures that need to be addressed in the stakeholder's port security management plan to ensure continuity of operations.

3.4.3 Mitigation strategies

The management plan should address the specific processes that will be implemented to prevent, protect the integrity of the supply chain, and restore the system as quickly as possible back to operational status after each occurrence. At all times the supply chain cargo must be protected during the response to the incident. Plans should be in place to move any cargo in the path of the fire, switch to back up systems for any security systems affected by the fire, and assign/reassign any additional staff to physically monitor and safeguard the access to the supply chain and critical protection systems during the incident. The mitigation plans should be in sufficient detail to describe the specific roles, responsibilities and steps to be taken by the stakeholders for implementing prevention procedures and the procedures that will be followed in response to an incident. The plan must address the expected delays and security systems down time that impact seaport operations and what procedures will be implemented to ensure supply chain security will be maintained during this interim by the seaport.

3.4.4 Recovery guidelines

The security management plan should provide specific steps that can be measured and assessed to determine the ability of the seaport to safeguard the supply chain and resume normal operations. If the port facility will be out of commission for an extended period, then a work around plan will have to be implemented to divert the normal upstream and downstream supply chain traffic to other locations. For any damaged systems, there must be an inspection and certification process that validates that replacement systems are operation properly. The security management plan must provide for alternative protection systems to replace any automated security protection systems that are out of commission and cannot protect the supply chain cargo. Manual systems, additional security guards and temporary secure storage areas with properly trained staff should be addressed in the plan as a temporary fix to support the continued flow of goods through the port until automated systems and normal operations can be restored.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

3.5 Stakeholder financial risks

3.5.1 Nature of risks

The financial well being of the stakeholders involved in seaport operations will have to be monitored and evaluated based on their ability to meet their specific roles and responsibilities for protecting the integrity of the supply chain and supporting port operations. Financial stress to the port stakeholders has the potential to impact a number of areas including having sufficient trained staff on hand, maintenance and spare parts provisioning, and security oversight and protection. Budget constraints have the potential to affect the quality and effectiveness of security provisions required to protect the supply chain, as well as the necessary provisions to maintain the level of services needed to ensure uninterrupted continuous operations of the supply chain. The seaport stakeholders must be able to protect the growing list of risks and threats to the supply chain, which may require the acquisition of additional security equipment and personnel to mitigate these threats and risks. In addition, unexpected costs because of random events

such as accidents, fires, damaging storms, criminal, and terrorist activities may severely affect financial ability of the stakeholders to support supply chain operations.

The financial impact of responding to new threats and risks as well as random events must be addressed in the management plan. If potential deficiencies are identified that may impact the security protection of the supply chain, then the plan must address what mitigation steps will be taken by the stakeholders to alter port operations to protect the cargo under their direct control.

3.5.2 Risk assessment

The seaport security management plan will need to have procedures for monitoring and evaluating the financial status of each stakeholder involved in the protection, processing and transporting of supply chain cargo entering and leaving the port. Their specific roles and responsibilities will have to be evaluated to identify single points of failure that could affect security and the delivery of goods if they are unable to provide the required services for safeguarding the integrity of the supply chain and port operations.

Any single point of failure will have to be determined and an assessment made to the expected impact on security and operations. Budget constrain will have to be analysed to determine their impact on current and future operations and what steps will need to be taken to maintain the required level of security and operational readiness of the seaport. Special attention must be paid to upstream operations where financial issues may impact their ability to implement the proper security provisions and oversight specified in ISO 28000.

3.5.3 Mitigation strategies

The security management plan must be able to evaluate and estimate where potential financial issues will impact the operations at the seaport. For those critical single points of failure, alternatives must be put in place that ensures continuity of the required supply chain security and operational services. The mitigation strategy must include a sound financial planning and budget forecasting process built into the plan with scheduled financial reviews to ensure that funds are in place to support the supply chain operational requirements. If deficits are identified in critical support areas, then specific steps must be addressed that produce acceptable work a rounds and/or reductions in non-critical services that do not comprise the integrity of the supply chain.

Upstream stakeholder financial issues that affect the security of delivered goods to the seaport will have to be addressed especially if it will require additional resources to be assigned to protect the integrity of the cargo entering the port. If the cost of the added resources exceeds the expected return on investment for handling the cargo, then the consideration may have to given to refusing the cargo until assurances are given that the cargo handling procedures are in conformance with ISO 28000 and the ISO 28004 series.

3.5.4 Recovery guidelines

The security management plan should provide specific steps that can be measured and assessed to determine the ability of the seaport to safeguard the supply chain and resume normal operations. If the port stakeholders are financially unable to adequately meet their supply chain support roles and responsibilities, then the plan must address alternative steps to ensure the security and operational status of the seaport. The plan should contain an audited operational budget that baselines the required financial resources to meet the security and supply chain continuity of operations tempo to support the expected flow of goods through the seaport.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

3.6 Labour related risks

3.6.1 Nature of risks

The security of the supply chain is largely dependant on the quality and quantity of the personnel assigned to protect the cargo while in port. Security staff must be fully trained to provide the specific security tasks in accordance with the roles and responsibilities assigned to them in the Supply Chain Security Management Plan. Any risk that causes a shortage of assigned trained personnel to monitor, operate and implement the seaport security procedures will put the supply chain at risk. Labour issues that can affect the normal operations of the port need to be identified and procedures put in place to ensure continuous operations of the seaport security systems. Work stoppage caused by labour unrest (strike, work slowdowns), insufficient staff to support operations and/or poorly trained staff has the potential to jeopardize the security procedures designed to protect the flow goods through the port. Port staff will need to be knowledgeable, informed on current procedures, and fully trained in prevention and disaster recovery procedures. In addition, there must be contingency plans in place to provide access to additional staff resources to supplement the staffing needs in order to maintain critical operations at the port and protection of the supply chain.

3.6.2 Risk assessment

The protection of the supply chain and continuous operations of the port will be a function of the quality and quantify of sufficient trained staff to support port operations. Staffing issues including labour unrest will have to be identified and assessed as to their impact on managing and implementing the port security procedures. For each critical staff position that could affect port and security operations, an assessment has to be made as to the vulnerability of the system if these staff resources are not available. The lost of key personnel for any reason (labour unrest, sickness, resignation) will have to be identified and contingency plans and procedures evaluated to determine their ability to ensure continuity of port and security operations. The assessment should address the expected delay time, the impact on security protection of the supply chain, and the required recovery procedures to return port operations to their normal operational status.

3.6.3 Mitigation strategy

To operate smoothly, the port security and operational plans must have sufficient and trained staff to support normal and any contingency operations brought on by the lost of key personnel. Specific procedures must be in place to provide for training of current and any replacement staff to support staff shortages caused by labour issues that could disrupt the flow of traffic and comprise the security of the supply chain. The management plan should address training of key staff to cover multiple roles and responsibilities in order to have sufficient knowledgeable staff on hand to minimizing the impact of labour issues and the possible disruptions that can be caused by the lack of staff resources. The plan must have back up plans for critical positions that if shortages occur in those areas, the flow and security of the supply chain will not be jeopardized.

3.6.4 Recovery guidelines

The security management plan should provide specific steps that can be measured and assessed to determine the ability of the seaport to safeguard the supply chain and resume normal operations. Staff shortages and/or poorly trained staff have the potential for jeopardizing the integrity of supply chain operations. Therefore, the plan must have provisions for acquiring additional trained resources on relatively short notice. The port stakeholders must be able to create a resource pool of trained and qualified staff covering each of the key positions that could affect operations if left vacant. In addition, the plan should address procedures for training and acquiring key replacement staff assigned to the resource pool.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

3.7 Mechanical/equipment breakdown risks

3.7.1 Nature of risks

Mechanical breakdown of major equipment items can slow down and/or bring operations to halt. Failure of port security and cargo protection systems will affect the integrity of the supply chain cargo. The cargo security and the continuity of operations will be affected if critical equipment is out of service for any extended period of time. Extended equipment and system failures could result in the reduction and/or stoppage of the scheduled flow of goods through the port if back up systems cannot be brought on line to support the normal flow of operations.

Equipment breakdown must include all port operational equipment from the loading crane, cargo transport vehicles, computer systems and seaport and supply chain security monitoring and protection systems. The failure of detection systems such as video surveillance, contra band scanning equipment, and software tracking database systems will force the slow down or stoppage of the movement of cargo through the port. The risk to the supply chain is high if failure of these systems leaves the supply chain cargo unprotected for any significant amount of time.

3.7.2 Risk assessment

The breakdown or loss of port and supply chain security protection systems and equipment can jeopardize the safety of the supply chain cargo. If backup or alternative protection systems cannot be brought on line quickly, then the processing and movement of cargo should be stopped until the protection systems are operational. The integrity of the supply chain is dependant on an uninterrupted continuous security shield that provides end-to-end protection of the cargo while in transit to its final destination. The risk to the supply chain can be considered high at any time that security provisions are out of commission. When these protections systems are out of commission, the movement of cargo should be halted and additional physical security systems implemented to safeguard the cargo until the port security systems can be brought back online. The port security management plan must address these contingencies and provides a reporting system that documents the break in protection and steps taken to certify that no breeches in security occurred during this period.

3.7.3 Mitigation strategies

To ensure continuous protection of the supply chain cargo, plans should be in place to provide additional physical manual security protection until any affected automated protection systems are restored to operational status. If the equipment/systems are off line for any extended period, then there must be provisions for shutting down the movement of cargo until back up systems and operational steps are in place to safeguard the supply chain and validate that the cargo has not been compromised while the systems were out of service. The mitigation strategies need to address preventive maintenance plans to keep equipment and systems operating at their full potential and contingency plans to provide alternative operations when unexpected equipment/system failures occur.

A preventive maintenance plan must be a key element of the mitigation strategy. An established Preventive Maintenance plan and knowledge of mean time between failure (MTBF) rates and mean time to repair (MTTR) times must be considered in determining how to minimize the impact of equipment/systems failures on continuous operations. Equipment and systems reaching their expected MTBF should be serviced or replaced to avoid unexpected breakdowns. The MTTR equipment repair times will determine the expected down times and what recovery strategies need to be in place to restore the systems to operational status. Matching maintenance schedules with scheduled down time between cargo handling requirements will allow for limited disruptions of the flow of traffic within the port.

3.7.4 Recovery guidelines

The security management plan should provide specific steps that can be measured and assessed to determine the ability of the seaport to safeguard the supply chain and resume normal operations. If the port security systems are offline and cannot ensure protection of the cargo, then plans must be in

place to stop port operations until the system can be restored. Back up systems and equipment must be readily available and staff trained to implement them once a system failure is determined. Where those automated systems will require an extended time to repair affecting the continuity of operations, manuals procedures and guidelines must be addressed by the security recovery plan to protect the supply chain until all security systems are operational. For any replacement and/or repaired port security systems, there must be an inspection and certification process that validates that replacement systems are operating properly providing the required security protection services.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

3.8 Political and governmental risks

3.8.1 Nature of risks

Political issues, changes in local government leadership and policies can have a direct impact on port operations, stakeholders and how security provisions are implemented at the port. Government regulations can affect how the ports will be governed, how the ports will operate and what agencies will be empowered to safeguard the supply chain. These changes could affect or restrict port ownership, require changes in customs and inspection procedures, and limit funding for port security and law enforcement support. The port security management plan should have designated roles and responsibilities for each of the stakeholders that govern port operations and provide security protection for the supply chain. Politically driven changes and/or restrictions to the organizational reporting structure and stakeholders' critical roles and responsibilities have the potential to affect continuity of operations and supply chain security.

In addition, the plan must address those changes imposed by international governments and governing bodies (EU, WTO, WCO, USA, NATO) that directly affects supply chain operations and security protection requirements. With the growing concerns over world wide terrorist and criminal activities, international governments, organizations, shippers and end users are demanding enhanced procedures for detecting and preventing contra-band (WMD materials, drugs) from entering the transportation systems and ports. Political driven changes, which could affect the capability of the port operators to ensure the uninterrupted protection of the supply chain, must be addressed.

3.8.2 Risk assessment

Policies and regulations that affect stakeholders and agencies empowered to support port operations and protect the supply chain, will have to be addressed and an assessment made to determine the level of risk imposed by the required changes. For each identified change in local and international government policies and regulations, an assessment has to be made on the capability of the seaport stakeholders to implement the changes and minimize any risks associated with the change. Changes in governing the supply chain protection requirements can severely affect how the supply chain is protected and can increase operational risks if the changes are not implemented properly. Government imposed regulations requiring additional security provisions can affect the continuity of operations and the resources (staff, equipment, funding) needed to safeguard the supply chain. New regulations such as increased scanning of cargo for contraband and weapons of mass destruction (WMD) may require additional detection equipment, facilities and staff trained in the use and maintenance of the equipment.

Each identified change will require an assessment on the capabilities of the assigned stakeholders to implement the change. Those changes determined to be mid to high risk, will require the port security plan to address specific mitigation steps to minimize the risk associated with the required change.

3.8.3 Mitigation strategies

The management plan should address the specific processes that will be implemented if changes in political and/or government policies and regulations affect the supply chain security protection provisions. For governmental policies that create risks to port operations and/or supply chain security,

the management plan should address what steps the stakeholders will take to implement the changes and minimized the risk to the system. Specific policies that change stakeholder roles and responsibilities will have to be addressed in the management plan with contingency steps outlined to ensure uninterrupted security protection for the supply chain.

Political/Policy changes that affect staffing either to replace or take on new responsibilities will have a training element that must be addressed in the management plan. The risk to the system will be the required leaning curve associated with any policy changes that affect the existing security provisions implemented at the seaport. The introduction of new requirements must be tested, validated and monitored to ensure that they are operating as required, do not add additional risk to the system, and provide any added security as envisioned by the change.

3.8.4 Recovery guidelines

The seaport security management plan must provide specific steps to implement any required Governmental policy changes that affect seaport and supply chain security operations. Recovery steps should include any changes in governance, staffing and/or implementation and operation of new security procedures, equipment and systems. The security management plan should provide specific steps that can be measured and assessed to determine the ability of the seaport to safeguard the supply chain and resume normal operations once any changes are implemented. For any new port security protection policies and/or systems, there must be an inspection and certification process that validates those policies and systems are operating properly providing the required security protection services.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

3.9 Terrorist risks

3.9.1 Nature of risks

Terrorist attacks are a worldwide global terrorist threat that materializes in many forms and no location is immune from these attacks. The random nature of the attacks are difficult to anticipate and often very difficult to detect. Terrorist activities are designed to disrupt and destroy operations, including physical damage to facilities, people and now the threat of cyber attacks that can disrupt computer operations, communications and security networks. Damages to the port facilities could include equipment, loading cranes, docking facilities, cargo and ships entering the ports. A secondary threat is the discovery of dangerous cargo containing weapons of mass destruction (WMD) and other bomb making materials that would require the shutting down of the port until these materials can be safely removed. Either instance can severely affect port operations and could have a long term effect in future operations if port facilities are damaged.

3.9.2 Risk assessment

Terrorist activities have the potential to shut down the port for indefinite periods and disrupt the integrity of the supply chain. Small and mid size seaports may have limited resources to detect and protect port operations from targeted terrorist activities. The smaller feeder type ports are especially vulnerable to problems with dangerous cargo that typically enters the supply chain at these feeder ports from local ground and rail cargo traffic. While the probability of a targeted terrorist activity is low at these smaller ports, any incident will have the potential of shutting down the port and creating a sufficient lost of traffic through the port that may not return once the port operations are restored if the user community views the port at a potential risk to future operations.

The protection of the supply chain and continuous operations of the port will be a function of the quality and quantify of sufficient trained staff to monitor and detect possible threats to the supply chain and port operations. The assessment should address the possibility of occurrence, provision in place to monitor and detect possible terrorist threats, and specific roles and responsibilities that will be followed by each stakeholder organization and agency once a threat is identified and/or detected at the seaport.

Special consider must be given to the growing threat of cyber attacks to the data and communications systems protecting the supply chain. Hacking of security systems that allow data and systems to be compromised by assessing security protection plans, corrupting critical data files and/or falsifying shipping data to hide dangerous cargo must have computer and network firewall detection systems in place to detect and prevent these attacks. A detailed assessment of the quality and capability of installed computer and network protection systems must be made to determine the vulnerability of the systems to possible cyber attacks.

3.9.3 Mitigation strategy

The mitigation strategy must address the need for detection, protection for critical seaport facilities and security systems, and planned prevention responses once any terrorist activities are discovered. Early detection and prevention steps are the best safeguards against random and well-planned acts of terrorism. Terrorism is a global issue and port stakeholders will need to establish links to global, regional and local law enforcement and Intelligence agencies in order to get information and intelligence alerts on any know terrorist activities that are focused in their areas.

Terrorist activities by definition will be secretive, covert operations that will require the ports to relay on those intelligence-gathering organizations to provide early warnings and alerts on any potential activities aimed at the supply chain and seaport operations. The security management plan must establish links to those agencies and establish well-documented procedures for detecting and responding to a potential terrorist attack. Specifically, the management plans should include at a minimum the following mitigation steps:

— Established links to intelligence and law enforcement agencies that track terrorist activities.

— Documented procedures on how to respond once a potential threat is identified.

— Use of technology equipment and systems to monitor port facilities and detect possible terrorist activities.

— Inspection and cargo scanning equipment to detect WMDs and dangerous materials hidden in cargo being shipped through the port.

— Documented procedures in place to handle the discovery of dangerous cargo for detaining, isolating and disposing of cargo to quickly return the port to normal operations.

— Continuous training to improve staff awareness on observing and detecting potential terrorist threats.

— Port access security procedures for positive identification of staff and visitors and protection barriers against unauthorized car and truck traffic attempting to enter port facilities.

In addition, the plan must have a clear understanding of the roles and responsibilities for each of the stakeholders in the monitoring, detection, data sharing and responding to possible threats. There must be provisions for periodic training sessions to test the responsiveness of the systems stakeholders, security detection systems and recovery steps in response to an incident.

3.9.4 Recovery guidelines

Everything must be done to detect and prevent a terrorist attack. Recovery could be extensive if major elements of the port are damaged. In addition, shippers will lose confidence in the port if the threat of terrorist activity is high. Any actual incident, once the port is back to normal operational status, will require an extensive amount of marketing to restore the level of confidence and integrity of the services being offered by the port to safeguard the supply chain. The quality of the recovery plan will be assessed in accordance with ISO 28000 and the ISO 28004 series, evaluated on its ability to ensure continuity of operations at the seaport and assigned a confidence number based on the assessment criteria.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

3.10 Weather related risks

3.10.1 Nature of risks

Extreme weather conditions may affect the capability of the port operators to safely load and upload ships, move cargo around the seaport and secure the cargo if security protection systems are comprised by the weather (lost of power, low visibility, and blocked access to secured areas). Weather predictions for seaport operations usually provide sufficient early warning that preventive steps can be taken to minimize the impact of major storms and/or inclement weather conditions that will bring port operations to a standstill. Based on geographical location and historical weather patterns, it is expected that over the course of the year, the seaport will experience some type of operational delays caused by rain, snow, ice, high winds and in some cases floods. These conditions in addition to extremely low and high temperatures will affect to some degree the flow of traffic at the seaport as well as the ability of the seaport to secure cargo if security systems are put out of commission by the weather conditions.

The management plan must have well documented plans for dealing with extreme weather conditions, which can compromise the security of the cargo being handled by the port. Weather conditions that shut down port operations and damage critical equipment, security systems and facilities will have to be addressed using historical data on the probability of occurrence and what steps have been taken in the past to restore the port to normal operational status.

3.10.2 Risk assessment

Extreme weather has the potential to destroy port facilities and slow down the transfer of goods at the seaport. If security provisions at the seaport are affected, then the integrity of the supply chain could be compromised if alternate plans for protecting the supply chain goods are implemented properly. Major storms (rain, wind, snow) causing flooding, sea surge and wind damage to power lines, buildings and port equipment) will slow down and/or suspend operations at the port. Extreme cold weather resulting in seasonal ice blockage and freezing temperatures affecting equipment and personnel will have to be assessed to determine their individual potential risks to continuous operations at the port and the ability of port personnel to manage the required supply chain security provisions to protect cargo at the port.

Each one of these possible risks has a probability of occurrence based on the historical weather patterns for each port geographical. While predictable to some degree, the security plans must address and assess those risk factors that would render the port unable to maintain positive security oversight and protection of the supply chain. Specifically, the risks associated with the lost of power and any damage to software systems, critical port security protection and monitoring systems will have to be assessed, and mitigation plans put in place to minimize the risks to integrity of the supply chain.

3.10.3 Mitigation strategies

The management plan should address the specific processes that will be implemented to prevent major delays, protect the integrity of the supply chain, and restore the system as quickly as possible back to operational status after each occurrence. Proper weather forecasting should provide sufficient advanced notice of the threat of severe weather conditions that could disrupt port operations. Therefore as part of the management plan, there must be provisions for monitoring weather conditions and providing alerts to the stakeholders when weather conditions have the potential for disrupting services. Using historical weather data and impacts to port operations, the plan should address the expected delays during certain period of the year that could be attributed to each weather condition and what seaport operations and security procedures were implemented to minimize the impact to the supply chain.

For those conditions such as seasonal cold and ice that affect port operations and security systems, the plan must address alternate provisions to ensure continuity of operations and protection of the supply chain. Depending on the severity of the pending weather, predetermined plans, procedures and

processes should be addressed in the management plan and staff trained on the necessary steps that needed to be taken to safeguard the supply chain. The mitigation plans should be in sufficient detail to describe the specific roles, responsibilities and procedures to be taken by the stakeholders for implementing prevention procedures that will be followed in response to pending weather conditions.

3.10.4 Recovery guidelines

Weather conditions affecting the supply chain and port operations are fairly predictable and typically provide enough advanced warning to take preventive measures to the protect the supply chain. Historical data on severe weather conditions, prevention steps and recovery procedures should be documented and reviewed to determine the best recovery steps to ensure continuity of operations. In all cases, critical systems that could affect port operations and security of the supply chain should have back up systems/equipment identified and staff trained to implement those recovery steps. Recovery could be extensive if major elements of the port and security are damaged and rendered inoperable for long periods on time.

The quality of the recovery plan will be assessed in accordance with ISO 28000, evaluated on its ability to ensure continuity of supply chain security protection operations at the seaport, and assigned a confidence number based on the assessment criteria.

4 Seaport security plan evaluation criteria and rating process

4.1 General

The evaluation process and security assessment of the Port Security Plan is the basis for determining conformance with the ISO International Standards and the capability of the installed security system to effectively safeguard the integrity of the supply chain cargo. To ensure conformance with the ISO 28000 security requirements, the Medium and Small seaport stakeholder organization security management plans should be periodically reviewed to determine the plan's capabilities and effectiveness in safeguarding the supply chain against the identified threats and risks to their seaport operations. The periodic review should examine the Port's security preparedness procedures for detecting, protecting and responding to incidents or emergency situations caused by security breaches and threats. The reviews conducted internally and by independent groups of trained security specialist, should be evaluated against a set of management, operational, risk mitigation and recovery performance indicators to establish a level of confidence that the seaport security plans are sufficient to safeguard the integrity of the supply chain for all cargo being handled by the seaport.

ISO 20858 provides for specific additional guidance and an established evaluation check list for measuring the capability and completeness of the Port Security Plan to address the threats and risks to the integrity of the supply chain. This document, when coupled with the appropriate clauses of ISO 20858, provides a set of comprehensive instructions and guidance that can be used to evaluate and determine if the implemented plans are in conformance with ISO 28000 and ISO 28004 series requirements and sufficient to protect the supply chain cargo while under port control.

4.2 Security plan evaluation process and procedures

The Medium and Small seaport stakeholders must develop and maintain a comprehensive security management plan documenting their procedures for safeguarding the integrity of the supply chain. The management plan will be audited and evaluated on a periodic basis to ensure that implemented security procedures are sufficient to safeguard the supply chain against the identified threats and risks to the seaport operations. The security protection plans will be evaluated against a set of performance metrics to determine the completeness, quality, and effectiveness of the seaport stakeholder developed plan in accordance with the requirements specified in ISO 28000. The evaluation will also include conformance with WCO SAFE Framework of Standards, the United States' Customs - Trade Partnership Against Terrorism (C-TPAT), and the European Commission's Authorized Economic Operator (AEO) Regulations.