Version 1b: September 5, 2009

ISO 28002: RESILIENCE IN THE SUPPLY CHAIN: REQUIREMENTS WITH GUIDANCE FOR USE

Draft Version 1b: September 5, 2009

Abstract

A comprehensive management systems approach to prevent, protect, prepare for, mitigate, respond to, and recover from disruptive incidents resulting in an emergency, crisis, or disaster.

NOTICE AND DISCLAIMER

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

FOREWORD

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2. The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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

ISO 28000 was prepared by Technical Committee ISO/TC 8, Ships and marine technology, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

0 INTRODUCTION

0.1 General

Companies and organizations across the globe are rapidly developing risk management and resilience programs in response to the risks posed by globalization. There is a strong demand for standards and best practices, as firms are seeking assurance that their suppliers and the extended supply chain have planned for, and taken steps to prevent and mitigate the threats and hazards to which they are exposed. To assure resilience in the supply chain, organizations must engage in a comprehensive and systematic process of prevention, protection, preparedness, mitigation, response, continuity and recovery.

The survivability of organizations within a supply chain depends largely on the resilience of their suppliers and customers. As result, incorporating resilience, and improving the resilience of an organization within the supply chain must be focused both within the organization and externally on its suppliers and customers.

This management system *Standard* (referred to as the "*Standard*") has applicability in the private, not-for-profit, non-governmental, and public sector environments. It is a management framework for action planning and decision making needed to anticipate, prevent if possible, and prepare for and respond to a disruptive incident (emergency, crisis, or disaster). It enhances an organization's capacity to manage and survive the event, and take all appropriate actions to help ensure the organization's continued viability. Regardless of the organization, its leadership has a duty to stakeholders to plan for its survival. The body of this document provides generic auditable criteria to establish, check, maintain, and improve a management system to enhance prevention, preparedness (readiness), mitigation, response, continuity, and recovery from disruptive incidents.

This *Standard* is designed so that it can be integrated with quality, safety, environmental, information security, risk, and other management systems within an organization. A suitably designed management system can thus satisfy the requirements of all these standards (see Annex B). Organizations that have adopted a process or systems approach to management systems (e.g., according to ISO 9001:2000, ISO 14001:2004, ISO 28000:2007 and/or ISO/IEC 27001:2005) may be able to use their existing management system as a foundation for the resilience management system as prescribed in this *Standard*.

The integrated adaptive, proactive, and reactive resilience approach can help avoid segregating or "siloing" risks, and provides an overall risk profile allowing the organization to better understand the relationships between risks and identify solutions to problems. It leverages the perspectives, knowledge, and capabilities of divisions and individuals within an organization. Because of the relatively low probability and yet potentially high consequence nature of many natural, intentional, or unintentional threats and hazards that an organization may face, an integrated approach allows an organization to establish priorities that address its individual needs for risk management within an economically sound context.

0.2 Supply Chain Environment

Managing risks in the supply chain requires an understanding of the organization's environment as well as the context of the global environment of the entire supply chain. Each node of the organization's supply change involves a set of risks and management processes of plan, source, make, deliver and return. All of these management processes should be included in an organization's overall resiliency program. With this understanding, an organization will define to which level, or tier in their supply chain to include in their resiliency program.

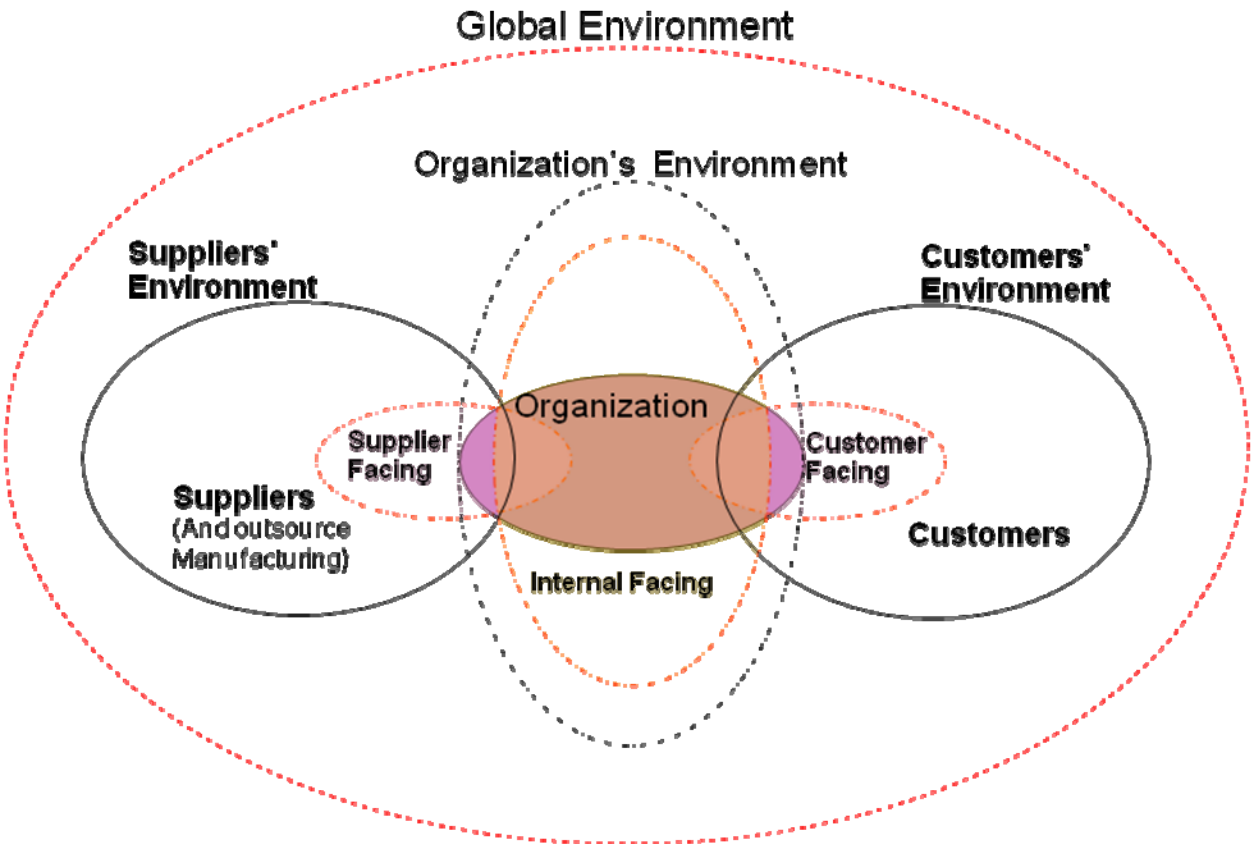

Figure 1: Resilience Management in the Supply Chain (Source: Supply Chain Council, 2007)

0.3 Process Approach

The management systems approach encourages organizations to analyze organizational and stakeholder requirements and define processes that contribute to success. A management system can provide the framework for continual improvement to increase the probability of enhancing security, preparedness, response, continuity, and resilience. It provides confidence to the organization and its customers that the organization is able to provide a safe and secure environment which fulfills organizational and stakeholder requirements.

This *Standard* adopts a *process approach* for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's resilience management system. An organization needs to identify and manage many activities in order to function effectively. Any

activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

The application of a system of processes within an organization, together with the identification and interactions of these processes and their management, can be referred to as a "process approach".

Figure 2 depicts the process approach for resilience management in the supply chain presented in this *Standard* encourages its users to emphasize the importance of:

a) Understanding an organization's risk, security, preparedness, response, continuity, and recovery requirements;
b) Establishing a policy and objectives to manage risks;
c) Implementing and operating controls to manage an organization's risks within the context of the organization's mission;
d) Monitoring and reviewing the performance and effectiveness of the resilience management system; and
e) Continual improvement based on objective measurement.

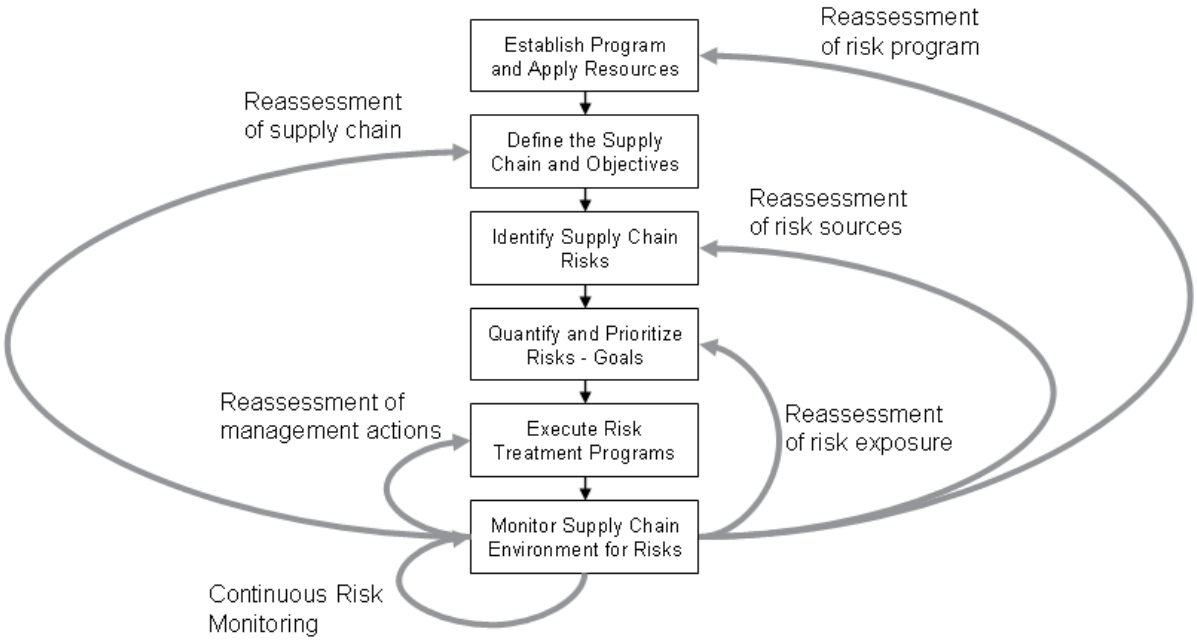

Figure 2: Process Approach for Resilience Management in the Supply Chain

0.2.1 Establish a Supply Chain Resiliency Program and Apply Resources

- Recognize supply chain risk management as a priority

- Secure executive support for the program and Secure resources necessary to execute the program

0.2.2 Define the Supply Chain and Resiliency Objectives

- Define the supply chain scope and Map the supply chain
- Define the objectives of managing risk in the subject supply chain

0.2.3 Identify Supply Chain Risks

- Comprehensively review the supply chain to identify risks
- Document identified risks to the extent possible

0.2.4 Quantify and Prioritize Risks

- Quantify each risk in terms of probability of occurrence and potential impact
- Use the quantification of the risks to prioritize the risks according to defined objectives

0.2.5 Execute Risk Treatment Programs

- Develop risk management actions consistent with each risk's priority
- Define each action's value in terms of reducing the probability and impact of the risk
- Develop and execute an implementation plan for the identified actions

0.2.6 Monitor Supply Chain Environment for Risks

- Continuously monitor the supply chain environment for risk events or precursors.
- When thresholds are triggered, execute applicable mitigation actions
- Document results for after action review and program improvement

0.2 "Plan-Do-Check-Act" (PDCA) model

This *Standard* adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure the Resilience management system processes. Figure 3 illustrates how a resilience management system takes as input the resilience management requirements and expectations of the interested parties and through the necessary actions and processes produces risk management outcomes that meet those requirements and expectations. Figure 3 also illustrates the links in the processes presented in clause 4.

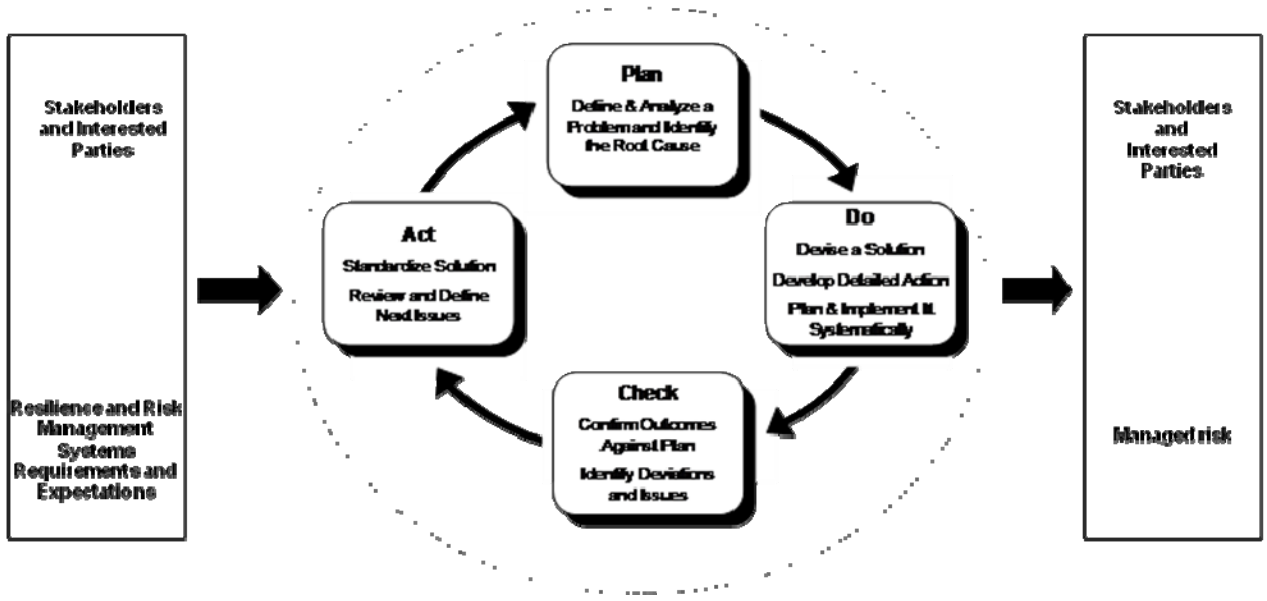

Figure 3: Plan-Do-Check-Act Model

Plan (establish the management system)	Establish management system policy, objectives, processes, and procedures relevant to managing risk and improving security, preparedness, mitigation, response, continuity, and recovery and to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the management system)	Implement and operate the management system policy, controls, processes, and procedures.
Check (monitor and review the management system)	Assess and measure process performance against management system policy, objectives, and practical experience and report the results to management for review.
Act (maintain and improve the management system)	Take corrective and preventive actions, based on the results of the internal management system audit and management review, to achieve continual improvement of the management system.

Compliance with this *Standard* can be verified by an auditing process that is compatible and consistent with the methodology of ISO 9001:2000, ISO 14001:2004, ISO 28000:2007 and/or ISO/IEC 27001:2005, and the PDCA Model.

ISO 28002: Resilience in the Supply Chain – Requirements with Guidance for Use

1. SCOPE

This *Standard* specifies requirements for a resilience management system to enable an organization to develop and implement policies, objectives, and programs taking into account legal requirements and other requirements to which the organization subscribes, information about significant risks, hazards and threats that may have an impact on it (and its stakeholders'), and protection of critical assets (human, physical, intangible, and environmental). This *Standard* applies to risks and/or their impacts that the organization identifies as those it can control, influence, or reduce, as well as those it cannot anticipate. It does not itself state specific performance criteria.

This *Standard* is applicable to any organization that wishes to:

a) Establish, implement, maintain, and improve a resilience management system;

b) Assure itself of its conformity with its stated resilience management policy;

c) Demonstrate conformity with this *Standard* by:

   i. Making a self-determination and self-declaration; or

   ii. Seeking confirmation of its conformance by parties having an interest in the organization (such as customers); or

   iii. Seeking confirmation of its self-declaration by a party external to the organization; or

   iv. Seeking certification/registration of its resilience management system by an external organization.

All the requirements in this *Standard* are intended to be incorporated into any type of organization's resilience management system. It provides all the elements required to integrate management, technology, facilities, processes, and people into the resilience culture, risk management, and resilience management system of an organization. The extent of the application will depend on factors such as the risk tolerance and policy of the organization; the nature of its activities, products, and services; and the location where, and the conditions in which, it functions.

This *Standard* provides generic requirements as a framework, applicable to all types of organizations (or parts thereof) regardless of size and nature of operation. It provides guidance for organizations to develop their own specific performance criteria, enabling the organization to tailor and implement a resilience management system appropriate to its needs and those of its stakeholders.

The *Standard* emphasizes resilience, the adaptive capacity of an organization in a complex and changing environment, as well as protection of critical assets. Applying this S*tandard* positions an organization to more readily prevent if possible, prepare for and respond to all manner of intentional,

unintentional, and/or naturally-caused disruptive events – which, if unmanaged, could escalate into an emergency, crisis, or disaster. It covers all phases of incident management before, during, and after a disruptive event.

This *Standard* enables an organization to:

a) Develop a prevention, protection, preparedness, mitigation and response/continuity/recovery policy;
b) Establish objectives, procedures, and processes to achieve the policy commitments;
c) Assure competency, awareness, and training;
d) Set metrics to measure performance and demonstrate success;
e) Take action as needed to improve performance;
f) Demonstrate conformity of the system to the requirements of this *Standard*; and
g) Establish and apply a process for continual improvement.

Annex A provides informative guidance on system planning, implementation, testing, maintenance, and improvement.

2. NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this *Standard*. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this *Standard* are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

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

NOTE: All documents below are available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

2.1 General Reference

ISO Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards.*

ISO 31000:2009, *Risk management – Principles and guidelines*

2.2 Parallel or Integrated Application of a Number of Systems

ISO 9001:2000, *Quality management systems — Requirements*.

ISO 14001:2004, *Environmental management systems – Requirements with guidance for use*.

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*.

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

3. TERMS AND DEFINITIONS

An extensive *Glossary* of terms appears in Annex D.

4. RESILIENCE MANAGEMENT SYSTEM REQUIREMENTS

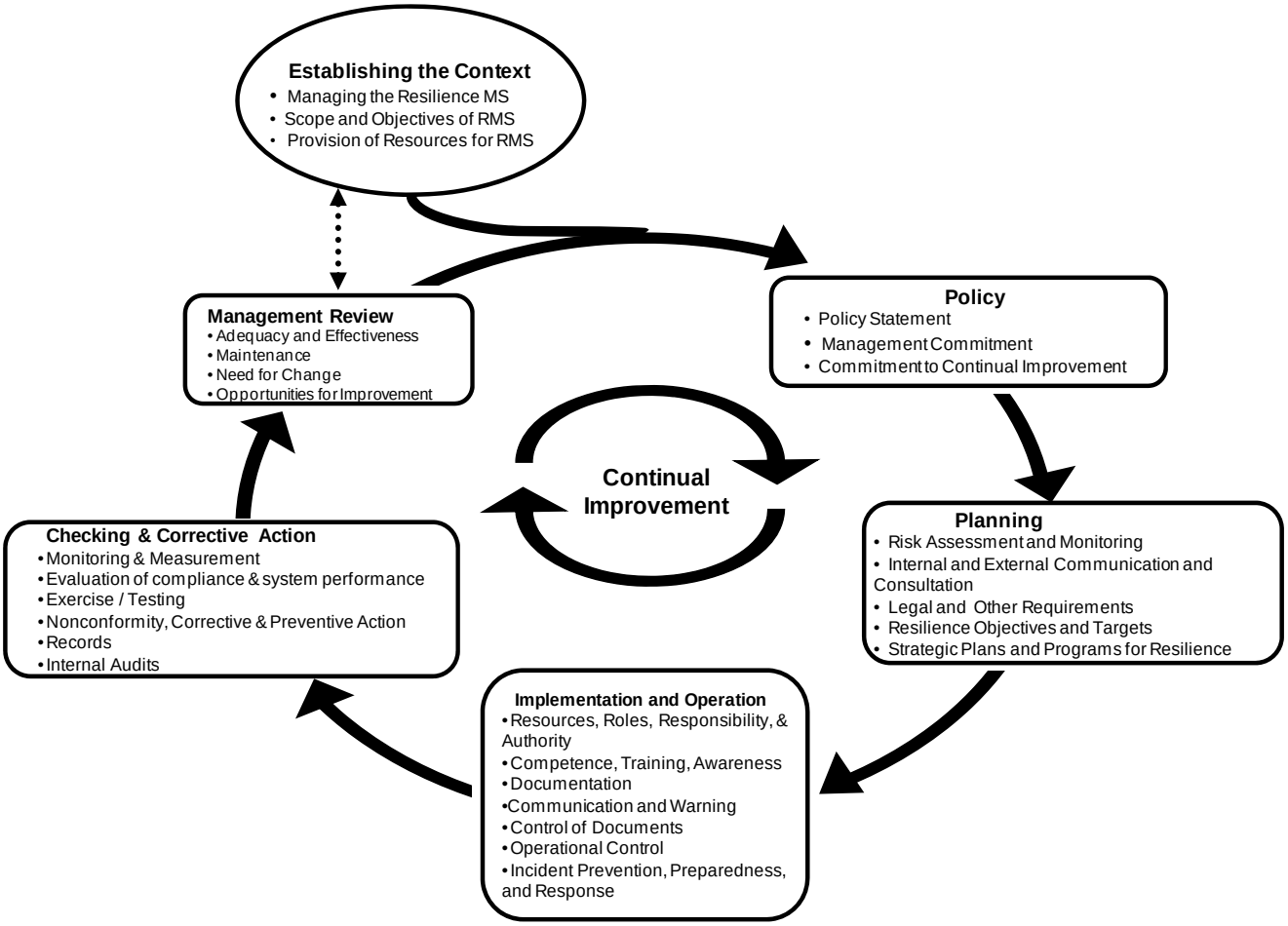

Figure 4: Resilience Management System Flow Diagram

4.1 General Requirements

The organization shall establish, document, implement, maintain, and continually improve a resilience management system in accordance with the requirements of this *Standard*, and determine how it will fulfill these requirements.

4.1.1 Understanding the Organization and its Context

The organization shall define and document the internal and external context of the organization.

The organization shall:

a) Determine the aspects of the organization's external context including:
    - the cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
    - supply chain tier, commitments and relationships;
    - key drivers and trends having impact on the objectives of the organization; and
    - perceptions and values of external stakeholders.
b) Determine the aspects of the organization's internal context including:
    - assets, activities, functions, services, products, partnerships, supply chains, and stakeholder relationships;
    - the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
    - information systems, information flows, and decision making processes (both formal and informal);
    - internal stakeholders;
    - policies, objectives, and the strategies that are in place to achieve them;
    - perceptions, values and culture;
    - standards and reference models adopted by the organization; and
    - structures (e.g. governance, roles and accountabilities).

The organization shall identify and document the following in defining the context for the management system and its commitment to the management of risk and resilience within specific internal and external contexts of the organization:

a) the organization's critical activities, functions, services, products, partnerships, supply chains, stakeholder relationships, and the potential impact related to a disruptive incident;
b) the components of end-to-end product or service supply chain flow, showing how they are configured or linked to deliver critical products and/or services;
c) links between the resilience management policy and the organization's objectives and other policies;
d) the organization's rationale for managing risk and resilience;
e) accountabilities and responsibilities for managing risk and resilience;
f) the organization's risk appetite or risk aversion;
g) resources available to assist those accountable or responsible for managing risk and resilience;
h) commitment to the periodic review and verification of the resilience management policy and framework; and
i) continual improvement.

4.1.2 Scope of Resilience Management System

The organization shall define and document the objectives and scope of its resilience management system within specific internal and external contexts of the organization.

In defining the scope, the organization shall:

a) Define the boundaries of the organization to be included in the scope of its resilience program, being the whole organization; one or more of its constituent parts; or the components of one or more end-to-end product or service supply chain flows.
b) Establish the requirements for resilience management, considering the organization's mission, goals, internal and external obligations (including those related to stakeholders), and legal responsibilities.
c) Consider critical operational objectives, assets, activities, functions, services, and products.
d) Determine risk scenarios, based both on potential internal and external disruptions, that could adversely affect the critical operations and functions of the organization within the context of their potential impact.
e) Define scope of the resilience management system in terms of and appropriate to the size, nature, and complexity of the organization from a perspective of continual improvement.

The organization shall define the scope consistent with protecting and preserving the integrity of the organization and its supply chain including relationships with stakeholders, interactions with key suppliers, outsourcing partners, and other stakeholders (for example, the organization's supply chain partners and suppliers, customers, stockholders, the community in which it operates, etc.).

A *Statement of Applicability* shall define the strategic weighting of security management, preparedness, mitigation, crisis management, emergency management, business continuity management, disaster management, and recovery management in developing the management system, based on the risk assessment and impact analysis (see 4.3.1).

NOTE: Organizations not in a supply chain situation may use this *Standard* to improve their organizational resilience by defining the boundaries of their resilience management system within the context of their individual organization.

4.1.3 Provision of Resources for the Resilience Management System

Management shall ensure the availability of resources essential for the implementation and control of the resilience management system. Resources include human resources and specialized skills, equipment, internal infrastructure, technology, information, intelligence, and financial resources.

4.2 Resilience Management Policy

Top management shall define, document, and provide resources for the organization's Resilience management policy reflecting a commitment to the protection of human, environmental, and physical assets; anticipating and preparing for potential adverse events; and business and operational resiliency.

4.2.1 Policy Statement

The policy statement of an organization shall ensure that within the defined scope of the resilience management system it:

a) Is appropriate to the nature and scale of potential threats, hazards, risks, and impacts (consequences) to the organization's activities, functions, products, services, and supply chain.
b) Includes a commitment to employee and community life safety as the first priority.
c) Includes a commitment to continual improvement.
d) Includes a commitment to enhanced organizational and supply chain sustainability and resilience.
e) Includes a commitment to risk avoidance, prevention, reduction, and mitigation.
f) Includes a commitment to comply with applicable legal requirements and with other requirements to which the organization subscribes.
g) Provides a framework for setting and reviewing resilience management objectives and targets.
h) Is documented, implemented, and maintained.
i) Makes reference to limitations and exclusions.
j) Determines and documents the risk tolerance in relation to the scope of the management system.
k) Is communicated to all appropriate persons working for or on behalf of the organization.
l) Is available to relevant stakeholders.

NOTE: An organization may choose to make public a non-confidential version of its policy not including sensitive security-related information.

m) Includes a designated policy ownership and/or responsible point of contact.
n) Is reviewed at planned intervals and when significant changes occur.
o) Is visibly endorsed by top management.

4.2.2 Management Commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the resilience management system by:

a) Establishing a resilience management system policy;
b) Ensuring that resilience management system objectives and plans are established;
c) Establishing roles, responsibilities, and competencies for resilience management;
d) Appointing one or more persons to be responsible for the resilience management system with the appropriate authority and competencies to be accountable for the implementation and maintenance of the management system;
e) Communicating to the organization the importance of meeting resilience management objectives and conforming to resilience management system policy, its responsibilities under the law, and the need for continual improvement;
f) Providing sufficient resources to establish, implement, operate, monitor, review, maintain, and improve the resilience management system;

g) Deciding the criteria for accepting risks and the acceptable levels of risk;
h) Ensuring that internal resilience management system audits are conducted;
i) Conducting management reviews of the resilience management system; and
j) Demonstrates its commitment to continual improvement.

4.3 Planning

4.3.1 Risk Assessment and Monitoring

The organization shall establish, implement, and maintain an ongoing formal and documented risk assessment process:

a) To identify risks due to intentional, unintentional, and naturally-caused hazards and threats that have a potential for direct or indirect impact on the organization's activities, operations, functions and supply chain; human, intangible, and physical assets; the environment; and its stakeholders;
b) To systematically analyze risk, vulnerability, criticality, and impacts (consequences);
c) To determine those risks that have a significant impact on activities, functions, services, products, supply chain, stakeholder relationships, and the environment (i.e., significant risks and impacts); and
d) To systematically evaluate and prioritize risk controls and treatments and their related costs.

The organization shall:

a) Document and keep this information up to date and confidential, as is appropriate;
b) Periodically review whether the resilience management scope, policy, and risk assessment are still appropriate given the organizations' internal and external context;
c) Re-evaluate risk and impacts within the context of changes within the organization or made to the organization's operating environment, procedures, functions, services, partnerships, and supply chains;
d) Develop risk criteria that are used to evaluate the significance of risk. The risk criteria reflect the internal and external context of the organization including its values, objectives and resources;
e) Establish criteria for maximum allowable downtime, recovery time objectives, as well as acceptable levels of losses associated with the organization and its supply chain's products, services and functions;
f) Establish a prioritized timeframe for recovery of activities and functions;
g) Evaluate the direct and indirect benefits and costs of options to reduce risk and enhance sustainability and resilience; and,
h) Ensure that the prioritized risks and impacts are taken into account in establishing, implementing, and operating its resilience management system.

4.3.1.1 Internal and External Communication and Consultation

The organization shall establish, implement, and maintain a formal and documented communication and consultation process with stakeholders and supply chain partners in the risk assessment process to ensure that:

a) threats, risks and impacts are adequately identified;
b) interests of stakeholders, as well as dependencies and linkages within the supply chain are understood;
c) resilience risk assessment process interfaces with other management disciplines; and
d) risk assessment is being conducted within the appropriate internal and external context and parameters relevant to the organization and its supply chain.

4.3.1.2 Monitoring and Reviewing the Risk Assessment Process

The organization shall establish, implement, and maintain a formal and documented process for monitoring and reviewing the risk assessment process to:

a) update risk assessment as needed;
b) identify and evaluate the impact on the risk assessment of the context, assumptions and other factors that may change over time due to internal and external circumstances; and
c) evaluate the effectiveness of risk controls and treatments.

4.3.2 Legal and Other Requirements

The organization shall establish and maintain (a) procedure(s):

a) To identify legal, regulatory, and other requirements to which the organization subscribes related to the organization's hazards, threats, and risks that are related to its facilities, activities, functions, products, services, supply chain, the environment, and stakeholders.
b) To determine how these requirements apply to its hazards, threats, risks and their potential impacts.

The organization shall document this information and keep it up to date.

The organization shall ensure that applicable legal, regulatory, and other requirements to which the organization subscribes are considered in developing, implementing, and maintaining its resilience management system.

4.3.3 Resilience Objectives and Targets

The organization shall establish, implement and maintain documented objectives and targets to manage risks in order to avoid, prevent, deter, mitigate, respond to, and recover from disruptive incidents. Documented objectives and targets shall establish internal and external expectations for the organization and its supply chain that are critical to mission accomplishment, product and service delivery, and functional operations.

Objectives shall be derived from and consistent with the resilience management policy and risk assessment, including the commitments to:

a) Risk avoidance, prevention, reduction, and mitigation;
b) Resilience enhancement through adaptive, proactive and reactive approaches;
c) Financial, operational and business requirements (including supply chain commitments);
d) Compliance with legal and other requirements; and
e) Continual improvement.

When establishing and reviewing its objectives and targets, an organization shall consider the legal, regulatory, and other requirements; its significant risks and impacts; its technological options; its financial, operational, and business requirements; and the views of stakeholders and other interested parties.

Targets shall be measurable qualitatively and/or quantitatively. Targets shall be derived from and consistent with the resilience management objectives and shall be:

a) to an appropriate level of detail;
b) specific, measurable, achievable, relevant and time-based (where practicable);
c) communicated to all relevant employees and third parties including contractors and supply chain partners with the intent that these persons are made aware of their individual obligations;
d) reviewed periodically to ensure that they remain relevant and consistent with the resilience management objectives and amended accordingly.

4.3.4 Strategic Plans and Programs for Resilience

The organization shall establish, implement and maintain one or more strategic program(s) for achieving its objectives and targets. The programs shall be optimized and prioritized in order to control and treat risks associated with threats and impacts of disruptions to the organization and its supply chain. The program(s) shall include:

a) Designation of responsibility and resources for achieving objectives and targets at relevant functions and levels of the organization;
b) Consideration of its activities, functions, regulatory or legal requirements, contractual and supply chain obligations, stakeholders' needs, mutual aid agreements, and the environment; and
c) The means and time-frame by which the resilience management objectives and targets are to be achieved.

The organization shall establish and maintain one or more strategic plans and program(s) for:

a) *Prevention and protection* - Avoid, eliminate, deter, protect, or prevent the likelihood of a disruptive incident and its consequences, including removal of human or physical assets at risk.
b) *Mitigation* - Minimize the impact of a disruptive incident.

c) *Response* - The initial response to a disruptive incident involving the protection of people and property from immediate harm. An initial reaction by management may form part of the organization's first response.
d) *Continuity* - Processes, controls, and resources are made available to ensure that the organization continues to meet its critical business and operational objectives.
e) *Recovery* - Processes, resources, and capabilities of the organization are re-established to meet ongoing operational requirements within the time period specified in the objectives.

The organization should evaluate its strategic program(s) to determine if these measures have introduced new risks. The resilience management programs shall be reviewed periodically to ensure that they remain effective and consistent with the objectives and targets. Where necessary the programs shall be amended accordingly.

4.4 Implementation and Operation

4.4.1 Resources, Roles, Responsibility, and Authority for Resilience Management

Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective resilience management, consistent with the achievement of its resilience management policy, objectives, targets and programs.

The organization's top management shall appoint (a) specific management representative(s) who, irrespective of other responsibilities, shall have defined roles, responsibilities, and authority for:

a) Ensuring that a resilience management system is established, communicated, implemented, and maintained in accordance with the requirements of this *Standard*;
b) Identifying and monitoring the requirements and expectations of the organization's supply chain partners and stakeholders and take appropriate action to manage these expectations;
c) Ensuring the availability of adequate resources; and
d) Reporting on the performance of the resilience management system to top management for review and as the basis for improvement.

The organization shall establish:

a) Resilience management, crisis management, and response team(s) with defined roles, appropriate authority, and adequate resources to oversee incident prevention, preparedness, response, and recovery;
b) Logistical capabilities and procedures to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities produced or donated to support the resilience management system;
c) Resource management objectives for response times, personnel, equipment, training, facilities, funding, insurance, liability control, expert knowledge, materials, and the time frames within which they will be needed from organization's resources and from any partner entities; and
d) Procedures for stakeholder assistance, communications, strategic alliances, and mutual aid.

The organization shall develop financial and administrative procedures to support the resilience management program before, during, and after an incident. Procedures shall be:

a) Established to ensure that fiscal decisions can be expedited; and
b) In accordance with established authority levels and accounting principles.

4.4.2 Competence, Training, and Awareness

The organization shall ensure that any person(s) performing tasks who have the potential to prevent, cause, respond to, mitigate, or be affected by significant hazards, threats, and risks are competent (on the basis of appropriate education, training, or experience) and retain associated records.

The organization shall identify competencies and training needs associated with management of its hazards, threats, and risks and its resilience management system, within the organization and its supply chain. It shall provide training or take other action to meet these needs and retain associated records.

The organization shall establish, implement, and maintain (a) procedure(s) to ensure persons working for it or on its behalf are aware of:

a) The significant hazards, threats, and risks, and related actual or potential impacts, associated with their work and the benefits of improved personal performance;
b) The procedures for incident prevention, deterrence, mitigation, self-protection, evacuation, response, continuity, and recovery;
c) The importance of conformity with the resilience management policy and procedures and with the requirements of the resilience management system;
d) Their roles and responsibilities in achieving conformity with the requirements of the resilience management system;
e) The potential consequences of departure from specified procedures; and
f) The benefits of improved personal performance.

The organization shall build, promote, and embed a resilience management culture within the organization and supply chain that:

a) Ensures the resilience management culture becomes part of the organization's and supply chain's core values and organization governance; and
b) Makes supply chain partners and stakeholders aware of the resilience management policy and their role in any plans.

4.4.3 Communication and Warning

With regard to its hazards, threats, and risks and resilience management system, the organization shall establish, implement, and maintain (a) procedure(s) for:

a) Documenting, recording, and communicating changes in documentation, plans, procedures, the management system, and results of evaluations and reviews;

b) Internal communication between the various levels and functions of the organization;
c) External communication with its supply chain and other partner entities and stakeholders;
d) Receiving, documenting, and responding to communication from external stakeholders;
e) Adapting and integrating a national or regional risk or threat advisory system or equivalent into planning and operational use;
f) Sharing intelligence with its supply chain and other partner entities and stakeholders;
g) Alerting stakeholders and supply chain partners potentially impacted by a potential, actual or impending disruptive incident;
h) Assuring availability of the means of communication during a crisis situation and disruption;
i) Facilitating structured communication with immediate and emergency responders;
j) Assuring the interoperability of multiple responding organizations and personnel;
k) Recording of vital information about the incident, actions taken, and decisions made; and
l) Operations of a communications facility.

The organization shall decide, based on life safety as the first priority and in consultation with supply chain partners and stakeholders, whether to communicate externally about its significant risks and impacts and document its decision. If the decision is to communicate, the organization shall establish and implement (a) method(s) for this external communication, alerts, and warnings (including with the media).

The resilience management communications systems shall be regularly tested.

4.4.4 Documentation

The resilience management system documentation shall include:

a) The resilience management policy, objectives, and targets;
b) Description of the scope of the resilience management system;
c) Description of the main elements of the resilience management system and their integration with related documents;
d) Documents, including records, required by this *Standard*; and
e) Documents, including records, determined by the organization to be necessary to ensure the effective planning, operation, and control of processes that relate to its significant risks.

The organization shall determine the security sensitivity of information and shall take appropriate steps to prevent unauthorized access.

4.4.5 Control of Documents

Documents required by the resilience management system and by this *Standard* shall be controlled. *Records* are a special type of document and shall be controlled in accordance with the requirements given in 4.5.4.

The organization shall establish, implement, and maintain (a) procedure(s) to:

a) Approve documents for adequacy prior to issue;

b) Review, update and re-approve documents as necessary;
c) Ensure that changes and the current revision status of documents are identified;
d) Ensure that relevant versions of applicable documents are available at points of use;
e) Establish document retention and archival parameters;
f) Ensure that original and archival copies of documents, data, and information remain legible and readily identifiable;
g) Ensure that documents of external origin determined by the organization to be necessary for the planning and operation of the resilience management system are identified and their distribution controlled;
h) Identify as obsolete all out-of-date documents that the organization is required to retain; and
i) Ensure the integrity of the documents by ensuring they are tamperproof, securely backed-up, accessible only to authorized personnel, and protected from damage, deterioration, or loss.

4.4.6 Operational Control

The organization shall identify those operations and activities that are necessary for achieving:

a) The resilience management policy;
b) The control of activities identified having significant risk;
c) Compliance with legal and regulatory requirements;
d) Its resilience management objectives;
e) The delivery of its resilience management programs; and,
f) The required level of supply chain resilience.

The organization shall establish, implement, and maintain adaptive and proactive plans and procedures for those operations that are associated with the identified significant risks, consistent with its resilience management policy, risk assessment, impact analysis, supply chain requirements, objectives, and targets, in order to ensure that they are carried out under specified conditions minimizing the risk, by:

a) Establishing, implementing, and maintaining procedures related to the identified hazards, threats and risks to the activities, functions, products, and services of the organization and communicating applicable procedures and requirements to its supply chain and contractors;
b) Establishing, implementing, and maintaining (a) documented procedure(s) to control situations where their absence could lead to deviation from the resilience management policy, objectives, and targets;
c) Evaluating any risks in upstream and downstream supply chain activities to establish, implement, and maintain (a) documented procedure(s) for minimizing the likelihood and/or mitigating the consequences of a disruptive incident;
d) Establishing and maintaining the requirements for goods and services which impact on resilience and communicating these to suppliers.
e) Stipulating the operating criteria in the documented procedures.

These procedures shall include controls for the design, installation, operation, refurbishment of resilience related items of equipment, logistical flows, instrumentation, etc. as appropriate. Where existing arrangements are revised and new arrangements introduced that could impact on the resilience management of operations and activities, the organization shall consider the associated risks before their implementation. The new or revised arrangements to be considered shall include:

a) Revised organizational structure, roles or responsibilities;

b) Revised resilience policy, objectives, targets and programs;

c) Revised process and procedures;

d) The introduction of new infrastructure, equipment or technology, which may include hardware or software;

e) The introduction of new contractors, suppliers, supply chain partners, or personnel, as appropriate.

The operational control procedures shall:

a) Address reliability and resiliency, the safety and health of people, and the protection of property and the environment potentially impacted by a disruptive incident;

b) Establish ownership of risk treatment and control measures (both internally and externally);

c) Ensure demand signals are comprehended in capacity planning;

d) Ensure processes are in place to validate supplier responses (e.g. validate site/process/product time to recover); and

e) Provide a feedback loop to know if past risk control strategies are changing as part of the routine engineering or process changes or a supplier's decision.

4.4.7 Incident Prevention, Preparedness, and Response

The organization shall establish, implement, and maintain (a) procedure(s) to manage disruptive incidents that can have (an) impact(s) on the organization, its activities, functions, services, supply chain, stakeholders, and the environment. The procedure(s) shall document how the organization will prevent, protect from, prepare for, mitigate, respond to and recover from disruptive incidents. The organization shall prepare for and respond to actual disruptive incidents to prevent the incident, minimize the likelihood of its occurrence, or mitigate associated adverse consequences.

When establishing, implementing, and maintaining (a) procedure(s) to prevent, prepare for and respond to a disruptive incident expeditiously, the organization should consider each of the following actions:

a) Preserve life safety;

b) Protect assets;

c) Prevent further escalation of the disruptive incident;

d) Reduce the length of the disruption to operations;
e) Restore critical operational continuity;
f) Recover normal operations (including evaluating improvements); and
g) Protect image and reputation (including media coverage and stakeholder relationships).

The organization shall periodically review and, where necessary, revise its incident prevention, preparedness, response, and recovery procedures – in particular, after the occurrence of accidents or incidents that can escalate into an emergency, crisis, or disaster.

The organization shall ensure that any person(s) performing incident prevention, protection, preparedness, mitigation, and response, and recovery measures on its behalf are competent on the basis of appropriate education, training, or experience, and retain associated records.

The organization shall document this information and updated it at a regular interval or as changes occur.

4.4.7.1 Prevention, Preparedness, and Response Structure

The organization shall establish, document and implement procedures and a management structure to prevent, prepare for, mitigate, and respond to a disruptive event using personnel with the necessary authority, experience and competence.

The prevention, preparedness and response structure shall provide for personnel to:

a) confirm the nature and extent of a disruptive event, or the potential impact the event may cause to the organization and its supply chain and stakeholders;
b) trigger appropriate proactive and reactive measures ;
c) have plans, processes and procedures for the activation, operation, coordination and communication of the prevention, preparedness and response measures;
d) have resources available to support the plans, processes and procedures to manage a disruptive event or work to minimize impact before realized; and
e) communicate with supply chain partner, stakeholders and local authorities, as well as the media.

4.4.7.2 Prevention, Protection and Mitigation

The organization shall establish, implement, and maintain procedures to prevent, protect from and mitigate a disruptive event and continue its activities based on resilience objectives developed through the risk assessment process. The procedures shall be based on a hierarchy of control measures in priority order that can be used to select and manage risk exposures, including procedures to:

a) Eliminate the risk by complete removal of the threat, or risk exposure;
b) Reduce the risk by modifying activities, processes, equipment or materials;

c) Isolation or separation of the risk from assets (physical or human);

d) Engineering controls to detect deter and delay a potential threat agent;

e) Administrative controls such as work practices or procedures that reduce risk; and

f) Protection of the asset if the risk cannot be eliminated or reduced.

4.4.7.3 Response

The organization shall establish, implement, and maintain procedures to manage a disruptive event and continue its activities based on recovery objectives developed through the risk assessment and impact analysis process. The organization shall document procedures (including supply chain arrangements) to ensure continuity of activities and management of a disruptive event, and shall be:

a) specific regarding the immediate steps that should be taken during a disruption;

b) flexible to respond to unanticipated threat scenarios and changing internal and external conditions;

c) focused on the impact of various threats that could potentially disrupt operations rather than specific events;

d) developed based on valid assumptions and an analysis of interdependencies; and

e) effective in minimizing consequences through implementation of appropriate mitigation strategies.

4.4.7.4 Continuity and Recovery Plans

The organization shall establish documented procedures that detail how the organization will manage a disruptive event and how it will recover or maintain its activities to a predetermined level, based on management-approved recovery objectives.

Each plan shall define:

a) purpose and scope;

b) objectives and measures of success;

c) implementation procedures;

d) roles, responsibilities and authorities;

e) communication requirements and procedures;

f) internal and external interdependencies and interactions;

g) resource requirements; and

h) information flow and documentation processes.

The organization shall periodically test, review and, where necessary, revise its continuity and recovery plans, in particular, after the occurrence of the disruptive event and its associated post event review.

4.5 Checking and Corrective Action

The organization shall evaluate resilience management plans, procedures, and capabilities through periodic assessments, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors should be reflected immediately in the procedures.

The organization shall keep records of the results of the periodic evaluations.

4.5.1 Monitoring and Measurement

The organization shall establish, implement, and maintain performance metrics and (a) procedure(s) to monitor and measure, on a regular basis, those characteristics of its operations that have material impact on its performance (including partnership and supply chain relationships). The procedure(s) shall include the documenting of information to monitor performance, applicable operational controls, and conformity with the organization's resilience management objectives and targets.

The organization shall evaluate and document the performance of the systems which protect its assets, as well as its communications and information systems.

4.5.2 Evaluation of Compliance and System Performance

4.5.2.1 Evaluation of Compliance

Consistent with its commitment to compliance, the organization shall establish, implement, and maintain (a) procedure(s) for periodically evaluating compliance with applicable legal and regulatory requirements.

The organization shall evaluate compliance with other requirements to which it subscribes including industry best practices. The organization may wish to combine this evaluation with the evaluation of legal compliance referred to above or to establish (a) separate procedure(s).

The organization shall keep records of the results of the periodic evaluations.

4.5.2.2 Exercises and Testing

The organization shall test and evaluate the appropriateness and efficacy of its resilience management system, its programs, processes, and procedures (including partnership and supply chain relationships).

The organization shall validate its resilience management system using exercises and testing that:

a) Are consistent with the scope of the resilience management system and objectives of the organization;
b) Are based on realistic scenarios that are well planned with clearly defined aims and objectives;
c) Minimize the risk of disruption to operations and the potential to cause risk to operations and assets;

d) Produce a formalized post-exercise report that contains outcomes, recommendations, and arrangements to implement improvements in a timely fashion;
e) Are reviewed within the context of promoting continual improvement; and
f) Are conducted at planned intervals, and from time to time on a non-periodic basis as determined by the management of the organization, as well as when significant changes occur within the organization and the environment it operates in.

4.5.3 Nonconformity, Corrective Action, and Preventive Action

The organization shall establish, implement, and maintain (a) procedure(s) for dealing with actual and potential nonconformity(ies) and for taking corrective action and preventive action. The procedure(s) shall define requirements for:

a) Identifying and correcting nonconformity(ies) and taking action(s) to mitigate their impacts;
b) Investigating nonconformity(ies), determining their cause(s), and taking actions in order to avoid their recurrence;
c) Evaluating the need for action(s) to prevent nonconformity(ies) and implementing appropriate actions designed to avoid their occurrence;
d) Recording the results of corrective action(s) and preventive action(s) taken; and
e) Reviewing the effectiveness of corrective action(s) and preventive action(s) taken.

Actions taken shall be appropriate to the impact of the potential problems, and conducted in an expedited fashion.

The organization shall identify changed risks, and identify preventive action requirements focusing attention on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment and impact analysis.

The organization shall make any necessary changes to the resilience management system documentation.

4.5.4 Control of Records

The organization shall establish and maintain records to demonstrate conformity to the requirements of its resilience management system and of this *Standard* and the results achieved.

The organization shall establish, implement, and maintain (a) procedure(s) to protect the integrity of records including access to, identification, storage, protection, retrieval, retention, and disposal of records.

Records shall be and remain legible, identifiable, and traceable.

4.5.5 Internal Audits

The organization shall conduct internal resilience management system audits at planned intervals, and from time to time on a non-periodic basis (as determined by the management of the organization) to determine whether the control objectives, controls, processes, and procedures of its resilience management system:

a) Conform to the requirements of this *Standard* and relevant legislation or regulations;
b) Conform to the organization's risk management requirements;
c) Are effectively implemented and maintained; and
d) Perform as expected.

An audit program shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency, and methods shall be defined. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.5.4), shall be defined in a documented procedure.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

4.6 Management Review

4.6.1 General

Management shall review the organization's resilience management system at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the resilience management system, including the resilience management system policy and objectives. The results of the reviews shall be clearly documented and records shall be maintained (see 4.5.4).

4.6.2 Review Input

The input to a management review shall include:

a) Results of resilience management system audits and reviews;
b) Feedback from interested parties;
c) Techniques, products, or procedures that could be used in the organization to improve the resilience management system performance and effectiveness;
d) Status of preventive and corrective actions;
e) Results of exercises and testing;
f) Vulnerabilities or threats not adequately addressed in the previous risk assessment;
g) Results from effectiveness measurements;

h) Follow-up actions from previous management reviews;
i) Any changes that could affect the resilience management system;
j) Adequacy of policy and objectives; and
k) Recommendations for improvement.

4.6.3 Review Output

The output from the management review shall include any decisions and actions related to the following:

a. Improvement of the effectiveness of the resilience management system;
b. Update of the risk assessment, impact analysis, and incident preparedness and response plans;
c. Modification of procedures and controls that effect risks, as necessary, to respond to internal or external events that may impact on the resilience management system, including changes to:
    i. Business and operational requirements;
    ii. Risk reduction and security requirements;
    iii. Operational conditions processes effecting the existing operational requirements;
    iv. Regulatory or legal requirements;
    v. Contractual obligations; and
    vi. Levels of risk and/or criteria for accepting risks.
d. Resource needs; and
e. Improvement to how the effectiveness of controls is being measured.

4.6.4 Maintenance

Top management shall establish a defined and documented resilience management system maintenance program to ensure that any internal or external changes that impact the organization are reviewed in relation to the resilience management system. It shall identify any new critical activities that need to be included in the resilience management system maintenance program.

4.6.5 Continual Improvement

The organization shall continually improve the effectiveness of the resilience management system through the use of the resilience management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review.

Annex A
(informative)

A GUIDANCE ON THE USE OF THE STANDARD

NOTE: The additional text given in this annex is strictly informative and is provided to assist in understanding the requirements contained in Section 4 of this Standard. While this information addresses and is consistent with the requirements of Section 4, it is not intended to add to, subtract from, or in any way modify those requirements.

A.0 Introduction

Natural disasters, environmental accidents, technology mishaps, and man-made crises have historically demonstrated that disruptive incidents can happen, impacting the public and private sectors alike. The challenge goes beyond most emergency response plans or disaster management activities previously deployed. Organizations now must engage in a comprehensive and systematic process of prevention, protection, preparedness, readiness, mitigation, response, continuity, and recovery. It is no longer enough to draft a response plan that anticipates disasters or emergency scenarios. Today's threats require the creation of an on-going, dynamic, and interactive process that serves to assure the continuation of an organization's core activities before, during, and after a major crisis event.

This *Standard* provides organizations of all sizes and types with the elements needed to achieve and demonstrate adaptive and proactive risk reduction and organizational resilience performance related to their physical facilities, services, activities, products, supply chains, and operational (business) continuity. They do so within the context of:

a) Increasing security risks and threats;
b) More stringent legislation and regulation;
c) More competitive business realities;
d) Increasing interdependencies in society (on an organizational, functional, or jurisdictional level);
e) Heightened awareness of the need for adequate emergency response and remediation planning;
f) Concerns of interested and affected parties; and
g) The need to assure operational continuity and resilience.

A disruptive incident not properly managed can rapidly escalate into an emergency, crisis, or even a disaster. Preparing for an incident before it occurs can minimize its likelihood and impact. An unmanaged disruptive incident can taint an organization's image, reputation, or brand in addition to resulting in significant physical or environmental damage, injury, or loss of life. This *Standard* provides a framework to aid organizations, and their supply chains, in successfully managing a disruptive incident by developing a strategy and action plan to safeguard its interests and those of its supply chain partners and stakeholders.

Adaptive and proactive planning and preparation for potential incidents and disruptions will diminish the likelihood, impact and length of the disruption. The holistic management process can help avoid

and minimize the suspension of critical services and operations, thereby allowing return to normal services and operations as rapidly as possible.

This *Standard* provides guidance or recommendations for any organization in the private, not-for-profit, and public sectors to identify and develop best practices to assist and foster action in:

a) Reducing risks throughout its supply chain;
b) Providing top management driven vision and leadership for strategies to protect assets and assure the resilience of the organization;
c) Identifying and evaluating assets, services, and functions to determine the parts of the operations and business that are critical to its short- and long-term success;
d) Identifying potential hazards and threats, and assessing risks and impacts;
e) Preventing and/or mitigating the impact of a wide variety of hazards and threats, including natural disasters, technological and environmental accidents, and man-made disasters (terrorism and crime);
f) Understanding the roles and responsibilities needed to protect assets and further resilience;
g) Managing necessary incident/emergency preparedness and response resources;
h) Developing strategic alliances and mutual aid agreements;
i) Developing and maintaining incident/emergency preparedness and response plans, and associated operational procedures;
j) Developing and conducting training and exercises to support and evaluate prevention, protection, incident/emergency preparedness, response plans, and operational procedures;
k) Developing and conducting training programs to implement preparedness, response plans, and operations procedures;
l) Ensuring that relevant employees, customers, suppliers, and other stakeholders are aware of the prevention, protection, incident/emergency preparedness and response arrangements and (where appropriate) have confidence in their application;
m) Developing internal and external communications procedures, including response to requests for information from the media or the public;
n) Establishing metrics for measuring and demonstrating success;
o) Documenting the key resources, infrastructure, tasks, and responsibilities required to support critical operational functions; and
p) Establishing processes that ensure the information remains current and relevant to the changing risk and operational environments.

It is simply good business for an organization to protect its physical, virtual, and human assets. The success of the management system depends on the commitment of all levels and functions in the organization, especially the organization's top management. Decision makers must be prepared to budget for and secure the necessary resources to make this happen. It is necessary that an appropriate administrative structure be put in place to effectively deal with prevention, mitigation, and management. This will ensure that all concerned understand who makes decisions, how the decisions are implemented, and what the roles and responsibilities of participants are. Personnel used for incident management should be assigned to perform these roles as part of their normal duties and not

be expected to perform them on a voluntary basis. Regardless of the organization – for profit, not for profit, faith-based, non-governmental – its leadership has a duty to stakeholders to plan for its survival.

A.1 General Requirements

The implementation of an organizational resilience (OR) management system specified by this *Standard* is intended to result in improved security, preparedness, response, continuity, and recovery performance. Therefore, this *Standard* is based on the premise that the organization will periodically review and evaluate its resilience management system to identify opportunities for improvement and their implementation. The rate, extent, and timescale of this continual improvement process are determined by the organization in the light of economic and other circumstances. Improvements in its resilience management system are intended to result in further improvements in security, preparedness, response, continuity, and recovery performance, and the organization's resilience. This *Standard* requires an organization to:

a) Establish an appropriate resilience management policy;
b) Identify the hazards and threats related to the organization's past, existing, or planned activities, functions, products, and services to determine the risk, consequences, and impacts of significance;
c) Identify applicable legal requirements and other requirements to which the organization subscribes;
d) Identify priorities and set appropriate resilience management objectives and targets;
e) Establish a structure and (a) program (s) to implement the policy and achieve objectives and meet targets;
f) Facilitate planning, control, monitoring, preventive and corrective action, and auditing and review activities to ensure both that the policy is complied with and that the resilience management system remains appropriate; and
g) Be capable of adapting to changing circumstances.

An organization with no existing resilience management system should establish its current position with regard to its critical assets and potential risk scenarios by means of a review or gap analysis. The aim of this review should be to consider all the organization's hazards and threats and their associated risks and impacts to critical assets as a basis for establishing the resilience management system.

The review should cover four key areas:

a) Identification of risks, including those associated with normal operating conditions, abnormal conditions including start-up and shut-down, and emergency situations and accidents.
b) Identification of applicable legal requirements and other requirements to which the organization subscribes.
c) Examination of existing risk management practices and procedures, including those associated with procurement and contracting activities.
d) Evaluation of previous emergency situations and accidents.

In all cases, consideration should be given to normal and abnormal operations and functions within the organization, its relationships with its supply chain and relevant stakeholders, and to potential disruptive and emergency conditions. Tools and methods for undertaking a review might include checklists, conducting interviews, direct inspection and measurement, or results of previous audits or other reviews, depending on the nature of the activities.

A.1.1 Understanding the Organization and its Context

In order for the organization to design and implement a resilience management system to manage its risks and that of its supply chain, the must first evaluate and understand the internal and external context in which it operates. When establishing the resilience management context, the organization should consider the internal and external parameters relevant to the organization and its supply chain. The context will determine the necessary scope and criteria for managing the risk to the organization and its supply chain as well as provide a basis for setting the risk assessment objectives, risk and recovery criteria, and parameters for the risk assessment and treatment processes.

A.1.2 Scope of Resilience Management System

An organization has the freedom and flexibility to define its boundaries, and may choose to implement this *Standard* with respect to the entire organization, to specific operating units of the organization or the components of one or more end-to-end product or service supply chain flows. The organization should define and document the scope of its resilience management system.

Scoping is intended to clarify the boundaries of the organization and nodes of the supply chain to which the resilience management system will apply, especially if the organization is a part of a larger organization at a given location. Once the scope is defined, all activities, products, and services of the organization within that scope need to be included in the resilience management system. In setting the scope, the credibility of the resilience management system will depend upon the choice of organizational boundaries. Where a part of an organization is excluded from the scope of its resilience management system, the organization should be able to explain the exclusion.

If this *Standard* is implemented for a specific operating unit, policies and procedures developed by other parts of the organization can be used to meet the requirements of this *Standard*, provided that they are applicable to the specific operating unit that will be subject to it.

Resilience management involves issues and actions before, during, and after a disruptive incident. Therefore, this *Standard* encompasses prevention, avoidance, deterrence, readiness, mitigation, response, continuity, and recovery. The risk environment, as well as business/operational realities, focuses different strategic weights on each of these components; however, no component should be weighted zero. The Statement of Applicability should elucidate the strategic weighting of security management, preparedness, emergency management, disaster management, crisis management, and business continuity management in developing the management system, based on the risk assessment and impact analysis (see 4.3.1).

A.1.3 Provision of Resources for the Resilience Management System

The resources needed for the resilience management system should be identified. These include human resources and specialized skills, equipment, internal infrastructure, technology, information, intelligence, and financial resources. Top management should ensure the availability of resources essential for the establishment, implementation, control and maintenance of the resilience management system.

A.2 Resilience Management Policy

The resilience management policy is the driver for implementing and improving an organization's resilience management system, so that it can maintain and enhance its sustainability and resilience. This policy should therefore reflect the commitment of top management to:

a) Comply with applicable legal requirements and other requirements;
b) Prevention, preparedness, and mitigation of disruptive incidents; and
c) Continual improvement.

The resilience management policy is the framework that forms the basis upon which the organization sets its objectives and targets. The resilience management policy should be sufficiently clear to be capable of being understood by internal and external interested parties (particularly its supply chain partners) and should be periodically reviewed and revised to reflect changing conditions and information. Its area of application (i.e., scope) should be clearly identifiable and should reflect the unique nature, scale, and impacts of the risks of its activities, functions, products, and services.

The resilience management policy should be communicated to all persons who work for (or on behalf of) the organization, including its supply chain and contractors working at an organization's facility. Communication to contractors can be in alternative forms to the policy statement itself, such as rules, directives, and procedures, and may therefore only include pertinent sections of the policy. The organization's resilience management policy should be defined and documented by its top management within the context of the resilience management policy of any broader corporate body of which it is a part and with the endorsement of that body.

It is essential that top management of the organization sponsors, provides the necessary resources, and takes responsibility for creating, maintaining, testing, and implementing a comprehensive resilience management system. This will insure that management and staff at all levels within the organization understand that the resilience management system is a critical top management priority. It is equally essential that top management engage a "top down" approach to the resilience management system; so that management at all levels of the organization understand accountability for effective and efficient plan maintenance as part of the overall governance priorities.

A resilience management planning team – including senior leaders from all major organizational functions and support groups – should be appointed to ensure wide-spread acceptance of the resilience management system.

A.3 Planning

4.3.1 Risk Assessment and Monitoring

The risk assessment process provides decision-makers with an improved understanding of the risks that could affect achievement of its objectives, and that of its supply chain. It is intended to create a systematic process for an organization to identify hazards, threats, risks, and impacts to determine those that are significant to the organization and its supply chain. The risk assessment provides a basis for evaluating the adequacy and effectiveness of current controls in place, as well as decisions on the most appropriate approaches to be used in managing and treating risks. It identifies those risks that should be addressed as a priority by the organization's resilience management system. The risk assessment provides the foundation for setting objectives, targets and programs within the management system, as well as measuring the efficacy of the resilience management system.

The risk assessment process is conducted within the internal and external context of the organization. Risk assessment is the overall process of risk identification, risk analysis and risk evaluation:

a) Risk identification: is the process of finding, recognizing and recording risks. It includes threat, criticality and vulnerability assessment as inputs into the identification process. The process considers the causes and sources of risks, as well as events, situations and circumstances that could impact the organization and its supply chain.

b) Risk analysis: is the process of developing and understanding of risk. It provides the decision-making basis for determining which risks should be treated and the most appropriate method for treating them. It considers the causes and sources of risk, their consequences and the likelihood that those consequences can occur.

c) Risk evaluation: is the process of comparing the estimated levels of risk with the risk criteria defined when the context was established. It determines the significance of the level and type of risk. The risk evaluation uses the understanding of the risk obtained in the risk analysis to make decisions about the strategies required for risk control and treatment.

Critical activities, functions, obligations, and processes should be identified and documented. Examples include purchasing, manufacturing, supply chain flows and nodes, sales, distribution, accounts receivable, accounts payable, payroll, information technology, and research and development. Once the critical processes and functions are identified, an analysis of each can be made using the risk criteria. Organizations may select categories of activities, products, and services to identify their criticality, risks, and impacts.

The risk assessment provides an understanding of risks, their causes, consequences, and their likelihoods. Therefore, an organization should conduct a comprehensive risk assessment within the scope of its resilience management system, taking into account the inputs and outputs (both intended and unintended) associated with:

a) Its current and relevant past activities, products, and services (internally and within the supply chain);

b) Planned or new developments, or new or modified activities, functions, products, and services;

c) Relations with supply chain partners and stakeholders;

d) Interactions with the environment and community; and

e) Critical infrastructure.

This process should consider normal and abnormal operating conditions, shut-down and start-up conditions, as well as reasonably foreseeable disruptive and emergency situations in order to set recovery time objectives and respond to recovery time requirements. However, it should be kept in mind that it is not possible to foresee all disruptive and emergency situations, so the organization must also consider the impact of a disruption on its critical assets, activities and function regardless of the nature of the disruption in order to set recovery time objectives and respond to recovery time requirements internally and within its supply chain.

There are many approaches and methodologies to risk assessment that will determine the order of the analysis steps adopted. Regardless of the methodology, the organization should have a formal and documented process for risk identification, risk analysis and risk evaluation that includes threat and hazard identification; and risk, vulnerability, criticality, consequence, and impact analysis.

The risk assessment should:

a) Give consideration to risks related to and criticality of the organization and its supply chain's activities, functions, products, and services and their potential for direct or indirect impact on the organization's operations, people, property, assets, compensation, image and reputation, profit, credit, and/or environment.
b) Use a documented quantitative or qualitative methodology to estimate likelihood or probability of the identified potential risks and significance of their impacts if they are realized.
c) Be based on reasonable criteria by giving due consideration to all potential risks it recognizes to its operations.
d) Consider its dependencies on others and others dependencies on the organization, including critical infrastructure and supply chain dependencies and obligations.
e) Consider data and telecommunications integrity and cyber security.
f) Evaluate the consequences of legal and other obligations which govern the organization's activities.
g) Consider risks associated with stakeholders, contractors, suppliers, and other affected parties.
h) Analyze information on risks, and select those risks which may cause significant consequences and/or those risks whose consequence is hard to be determined in terms of significance.
i) Analyze and evaluate the level of resilience of each hazard or threat and each critical asset.
j) Evaluate risks and impacts it can control and influence. (However, in all circumstances it is the organization that determines the degree of control and its strategies for risk acceptance, avoidance, management, minimization, tolerance transfer, and/or treatment.)

In some locations, critical infrastructure, societal assets, and cultural heritage may be an important element of the surroundings in which an organization operates, and therefore should be taken into account in the understanding of its risks and impact on surroundings.

Since an organization might have many risks and impacts, it should establish and document criteria and a methodology to determine those that it will consider significant. There is no single method for determining significant risks and impacts. However, the method used should provide consistent results

and include the establishment and application of evaluation criteria, such as those related to criticality of each organizational activity and function, legal issues, and the concerns of internal and external stakeholders. An organization should analyze likelihood and impacts of disruptions to its operations and identify critical operations that are given high priority for restoration, in order to set up recovery time objectives.

When assessing impacts the organizations should consider:

a) *Human cost*: Physical and psychological harm to employees, customers, suppliers, and other stakeholders.
b) *Financial cost*: Equipment and property replacement, downtime, overtime pay, stock devaluation, lost sales/business, lawsuits, regulatory fines/penalties, etc.
c) *Corporate image cost*: Reputation, standing in the community, negative press, loss of customers, etc.
d) *Economic losses to the community in which the organization operates*: Indirect impacts on the regional economy, reduction in the regional net economy, losses to the tax base of local jurisdictions, etc.
e) *Environmental impacts*: Degradation to the quality of the environment or to endangered species.

In estimating maximum allowable downtime, acceptable level of losses, and a prioritized timeframe for recovery, the organization's objectives should be based on:

a) It's supply chain commitments, considering upstream and downstream consequences;
b) How long processes can be nonfunctional before impacts become unacceptable.
c) How soon processes should be restored (shortest allowable outage restored first).
d) Different recovery time objectives according to time of year (year-end, tax filing, etc.).
e) Identifying and documenting alternate procedures for strategic alliance, mutual aid, manual workaround, notification/alert, etc.
f) Evaluation of costs of alternate procedures versus waiting for system to be restored.

When developing information relating to its significant risks and impacts, the organization should consider the need to retain the information for historical purposes, as well as how to use it in designing and implementing its resilience management system.

The process of identification and evaluation of risks and impacts should take into account the location of activities, cost and time of undertaking the analysis, and the availability of reliable data. Information already developed for business planning, regulatory, or other purposes may be used in this process.

This process of identifying and evaluating risks and impacts is not intended to change or increase an organization's legal obligations.

A.3.2 Legal and Other Requirements

The organization needs to identify the legal requirements that are applicable to activities and functions. These may include:

a) National and international legal requirements;

b) State/provincial/departmental legal requirements; and
c) Local governmental legal requirements.

Examples of other requirements to which the organization may subscribe include, if applicable:

a) Agreements with public authorities;
b) Agreements with customers;
c) Non-regulatory guidelines;
d) Voluntary principles or codes of practice;
e) Voluntary labeling or product stewardship commitments;
f) Requirements of trade associations;
g) Agreements with community groups or non-governmental organizations;
h) Public commitments of the organization or its parent organization; and/or
i) Corporate/company requirements.

The determination of how legal and other requirements apply to an organization's risk assessment is usually accomplished in the process of identifying these requirements. Therefore, it may not be necessary to have a separate or additional procedure in order to make this determination.

A.3.3 Resilience Objectives and Targets

The objectives and targets should be specific and measurable wherever practicable. An objective is an overall goal, consistent with the policy, that an organization sets itself to achieve. A target is a detailed performance requirement applicable to the organization (or parts thereof) that arises from the objectives and that needs to be set and met in order to achieve those objectives. They should cover short- and long-term issues. Programs should define the strategic means for achieving objectives and targets.

Objectives, targets, and program(s) should be based on the risk assessment.

When considering its technological options, an organization should consider the use of best available technologies where economically viable, cost-effective, and judged appropriate.

The reference to the financial requirements of the organization is not intended to imply that organizations are obliged to use cost-accounting methodologies; however, the organization may choose to consider direct, indirect, and hidden costs.

A.3.4 Strategic Plans and Programs for Resilience

The creation and use of one or more programs is important to the successful implementation of a resilience management system. Each program should describe how the organization's objectives and targets will be achieved, including timescales, necessary resources, and personnel responsible for implementing the program(s). This (these) program(s) may be subdivided to address specific elements of the organization's operations.

The program should include, where appropriate and practical, consideration of all stages of an organization's activities and functions related to supply chain obligations, planning, design, construction, commissioning, operation, retrofitting, production, marketing, waste disposal, and decommissioning. Program development may be undertaken for current and new activities, products, and/or services.

Prevention, preparedness, and mitigation programs should consider removal of people and property at risk; relocation, retrofitting, and provision of protective systems or equipment; information, data, document, and cyber security; establishment of threat or hazard warning and communication procedures; and redundancy or duplication of essential personnel, critical systems, equipment, information, operations, or materials, including those from partner agencies.

The organization should plan for incident response and recovery, taking into account core activities, supply chain and contractual obligations, employee and neighbouring community necessities, operational continuity, and environmental remediation. Organizations have different approaches to managing crises. Regardless of the approach, there are three generic and interrelated management response steps that require pre-emptive planning and implementation in case of a disruptive incident:

a) *Emergency response*: The initial response to a disruptive incident usually involves the protection of people and property from immediate harm. An initial reaction by management may form part of the organization's first response.
b) *Continuity*: Processes, controls, and resources are made available to ensure that the organization continues to meet its critical operational objectives.
c) *Recovery*: Processes, resources, and capabilities of the organization are re-established to meet ongoing operational requirements. This will often include the introduction of significant organizational improvements even to the extent of refocusing strategic or operational objectives).

A.4 Implementation and Operation (Tactical Implementation)

A.4.1 Resources, Roles, Responsibility, and Authority

The successful implementation of a resilience management system calls for a commitment from all persons working for the organization or on its behalf. Roles and responsibilities therefore should not be seen as confined to the risk management function, but can also cover other areas of an organization, such as operational management or staff functions other than risk management, security, preparedness, continuity, and response.

This commitment should begin at the highest levels of management. Accordingly, top management should establish the organization's resilience management policy, and ensure that the resilience management system is implemented. As part of this commitment, the top management should designate (a) specific management representative(s) with defined responsibility and authority for implementing the resilience management system. In large or complex organizations there may be more than one designated representative. In small or medium-sized enterprises, these responsibilities may be undertaken by one individual.

It is necessary that an appropriate administrative structure be put in place to effectively deal with crisis management during a disruptive incident. Clear definitions must exist for a management structure,

authority for decisions, and responsibility for implementation. An organization should have a Crisis Management Team to lead incident/event response. The team should be comprised of such functions as human resources, information technology, facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions, with all under the clear direction of top management or its representatives.

The Crisis Management Team may be supported by as many Response Teams as appropriate taking into account such factors as organization size and type, number of employees, location, etc. Response Teams should develop response plans to address various aspects of potential crises – such as damage assessment, site restoration, payroll, human resources, information technology, and administrative support. Response plans should be consistent with and included within the overall resilience management system. Individuals should be recruited for membership on Response Teams based upon their skills, level of commitment, and vested interest.

Management should also ensure that appropriate resources are provided to ensure that the resilience management system is established, implemented, and maintained. It is also important that the key resilience management system roles and responsibilities are well defined and communicated to all persons working for or on behalf of the organization.

Roles, responsibilities, and authorities should also be defined, documented and communicated for coordination with external stakeholders. This should include interactions with contractors, partners, organizations within the supply chain, public authorities, and financial institutions.

A.4.2 Competence, Training, and Awareness

The organization should identify the awareness, knowledge, understanding, and skills needed by any person with the responsibility and authority to perform tasks on its behalf. This *Standard* states that:

a) The importance of conformity with the resilience management policy and procedures and with the requirements of the resilience management system;
b) The significant hazards, threats, and risks, and related actual or potential impacts, associated with their work and the benefits of improved personal performance;
c) Their roles and responsibilities needed to achieve conformity with the requirements of the resilience management system;
d) The procedures for incident prevention, deterrence, mitigation, self-protection, evacuation, response, and recovery; and
e) The potential consequences of departure from specified procedures.

Awareness and education programs should be established for internal and external stakeholders, including supply chain partners, potentially impacted by a disruptive incident.

Awareness, knowledge, understanding, and competence may be obtained or improved through training, education, or work experience.

The organization should require that contractors working on its behalf are able to demonstrate that their employees have the requisite competence and/or appropriate training.

Management should determine the level of experience, competence, and training necessary to ensure the capability of personnel, especially those carrying out specialized resilience management functions.

All personnel should be trained to perform their individual responsibilities in case of a disruptive incident or crisis. They should also be briefed on the key components of the resilience management system, as well as the response plans that affect them directly. Such training could include procedures for preventions, protection and mitigation measures, evacuation, shelter-in-place, check-in processes to account for employees, arrangements at alternate worksites, and the handling of media inquiries by the company.

The Crisis Management and Response Teams should be educated about their responsibilities and duties including interactions with first responders, supply chain partners, and stakeholders. Checklists of critical actions and information to be gathered are valuable tools in the education and response processes. Teams should be trained regular intervals (at least annually), and new members should be trained when they join. These teams should also be trained with respect to prevention of incidents that may escalate into crises.

It is recommended that any external resources that may be involved in a response – such as Fire, Police, Public Health, and third-party vendors – should be familiar with relevant parts of the response plans.

A.4.3 Communication and Warning

Internal communication is important to ensure the effective implementation of the resilience management systems. Methods of internal communication may include regular work group meetings, newsletters, bulletin boards, and intranet sites.

Organizations should identify and establish relationships with public sector agencies, organizations, and officials responsible for intelligence, warnings, prevention, response, and recovery related to potential disruptions identified in the risk assessment. Arrangements should be made for communication and warnings internally and externally for normal and abnormal conditions.

Organizations should implement a procedure for receiving, documenting, and responding to relevant communications from it supply chain, stakeholders and interested parties. This procedure can include a dialogue with interested parties and consideration of their relevant concerns. In some circumstances, responses to interested parties' concerns may include relevant information about the risks and impacts associated with the organization's functions and operations. These procedures should also address necessary communications with public authorities regarding emergency planning and other relevant issues.

The organization may wish to plan its communication taking into account the decisions made on relevant target groups, the appropriate messages and subjects, and the choice of means. When considering external communication about hazards, threats, risks, impacts, and control procedures, organizations should take into consideration the views and information needs of all stakeholders. If the organization decides to communicate externally on its hazards, threats, risks, impacts, and control procedures, the organization should establish a procedure to do so. This procedure could change depending on several factors, including the type of information to be communicated, the target group, and the individual circumstances of the organization. Methods for external communication can include annual reports, newsletters, websites, warnings, and community meetings.

Effective communication is one of the most important ingredients in managing a disruption or crisis. Internal and external stakeholders should be identified in order to convey alerts, warnings, crisis, and organizational response information. In order to provide the best communications and suitable messages for various groups, it may be appropriate to segment the audiences. In this way, messages tailored specifically for a group can be released.

Preplanning for communications is critical. Draft message templates, scripts, and statements can be crafted in advance for threats identified in the risk assessment. Procedures to ensure that communications can be distributed at short notice should also be established, particularly when using resources such as an Intranet, Internet sites, and toll-free hotlines.

The organization should designate a single primary spokesperson (with back-ups identified) who will manage/disseminate crisis communications to the media and others. This individual should be trained in media relations prior to a crisis. All information should be funneled through a single source to assure that the messages being delivered are consistent. It should be stressed that personnel should be informed quickly regarding where to refer calls from the media and only authorized company spokespeople may speak to the media. In some situations, an appropriately trained site spokesperson may also be necessary.

A.4.4 Documentation

The level of detail of the documentation should be sufficient to describe the resilience management system and how its parts work together, and provide direction on where to obtain more detailed information on the operation of specific parts of the resilience management system. This documentation may be integrated with documentation of other systems implemented by the organization. It does not have to be in the form of a manual.

The extent of the resilience management system documentation can differ from one organization to another due to:

a) The size and type of organization and its activities, products or services;
b) The complexity of processes and their interactions; and
c) The competence of personnel.

Examples of documents include:

a) Statements of policy, objectives, and targets;
b) Information on significant risks and impacts;
c) Procedures;
d) Process information;
e) Organizational charts;
f) Internal and external standards;
g) Site response, mitigation, emergency, and crisis plans; and
h) Records.

Any decision to document (a) procedure(s) should be based on issues such as:

a) The consequences, including those to human and physical assets and the environment, of not doing so.
b) The need to demonstrate compliance with legal and with other requirements to which the organization subscribes.
c) The need to ensure that the activity is undertaken consistently.
d) The advantages of doing so, which can include:
    i. Easier implementation through communication and training.
    ii. Easier maintenance and revision.
    iii. Less risk of ambiguity and deviations.
    iv. Demonstrability and visibility.
e) The requirements of this *Standard*.

Documents originally created for purposes other than the resilience management system may be used as part of this system, and (if so used) will need to be referenced in the system.

A.4.5 Control of Documents

The intent of 4.4.5 is to ensure that organizations create and maintain documents in a manner sufficient to implement the resilience management system. However, the primary focus of organizations should be on the effective implementation of the resilience management system and on security, preparedness, response, continuity, and recovery performance and not on a complex document control system.

Organizations should ensure the integrity of the documents by ensuring they are tamperproof, securely backed-up, accessible only to authorized personnel, and protected from damage, deterioration, or loss.

A.4.6 Operational Control

An organization should evaluate those of its operations that are associated with its identified significant risks, and ensure that they are conducted in a way that will control or reduce the adverse impacts associated with them in order to fulfill the requirements of its resilience management policy and meet its objectives and targets. This should include all parts of its operations including supply chain and maintenance activities.

As this part of the resilience management system provides direction on how to take the system requirements into day-to-day operations, it requires the use of (a) documented procedure(s) to control situations where the absence of documented procedures could lead to deviations from the resilience management policy, objectives, and targets.

To minimize the likelihood of a disruptive incident, these procedures should include controls for the design, installation, operation, refurbishment, and modification of risk-related items of equipment, instrumentation, etc., as appropriate. Where existing arrangements are revised or new arrangements introduced that could impact on operations and activities, the organization should consider the associated minimization of threats and risks before their implementation.

A.4.7 Incident Prevention, Preparedness, and Response

It is the responsibility of each organization to develop incident prevention, preparedness, mitigation response, and recovery procedures that suits its own particular needs. In developing its procedures, the organization should include consideration of:

a) A potential disruptive incident should be identified, understood, and addressed and – in doing so – avoided or prevented. The risk assessment can be used to identify the specifics of potential disruptive incidents, including any precursors and warning signs.

b) Risk management should be a systematic and holistic process that builds on the formal risk assessment to identify, measure, quantify, and evaluate risks to provide the optimal solution.

c) Risk treatment options can include avoidance, elimination, reduction, spreading, transfer, and acceptance strategies. *Avoidance* and *elimination* can either evade activities that gives rise to the risk or remove the source of the risk. *Reduction* lowers the risk or the severity of the loss. *Spreading* distributes assets and/or the potential loss of capacity. *Transfer* involves sharing the risk with another party or parties. *Acceptance* is an informed decision to take a particular risk.

A.4.7.1 Prevention, Preparedness, and Response Structure

The organization should establish procedures to recognize when specific dangers are manifest that necessitate the need for some level of reaction to avoid, prevent, mitigate or respond to the potential disruption. A strong program of detection and avoidance policies and procedures will support this process.

- Certain departments or functions are uniquely situated to observe warning signs of an imminent crisis. Personnel assigned to these departments or functions should be trained appropriately. The responsibility to report a potential crisis (including the notification mechanism) should be communicated to all employees. The general employee population may also be an excellent source of predictive information when there is a documented reporting structure and where attention is paid to what the employee reports.

A potential disruptive incident, once recognized, should be immediately reported to a supervisor, a member of management, or another individual tasked with the responsibility of crisis notification and management internally and within the supply chain.

a) Specific notification criteria should be established, documented, and adhered to by all employees (with the timing and sequence of notification calls clearly documented). The actual activation of a reaction process should require very specific qualifications being met.

b) Qualified personnel should have ready access to the updated, confidential listings of persons and organizations to be contacted when certain conditions or parameters of a potential crisis are met.

c) Notifications in a disruptive or crisis situation should be timely and clear, and should use a variety of procedures and technologies – with recognition that devices used have advantages and limitations.

d) In some types of disruptions and crises, the notification systems are themselves impacted by the disaster, either through capacity issues or infrastructure damage. Thus, it is important to have redundancies built into the notification system, and several different ways to contact the listed individuals and organizations.

Problem assessment (an evaluative process of decision making that will determine the nature of the issue to be addressed) and severity assessment (the process of determining the severity of the disruption and what any associated costs may be in the long run) should be made at the outset of a disruption. Factors to be considered include the size of the problem, its potential for escalation, and the possible impact of the situation on the organization and its supply chain.

The point at which a situation is declared to be an emergency or crisis should be clearly defined, documented, and fit very specific and controlled parameters. Responsibility for declaring a crisis should also be clearly defined and assigned. First and second alternates to the responsible individual should be identified. The activities that declaring an emergency or crisis will trigger include, but are not limited to:

a) Notification of supply chain partners and other impacted parties;

b) Additional call notification;

c) Evacuation, shelter, or relocation;

d) Safety protocol;

e) Response site and alternate site activation;

f) Team deployment;

g) Personnel assignments and accessibility;

h) Emergency contract activation; and

i) Operational changes.

A.4.7.2 Prevention, Protection and Mitigation

Prevention can include proactive steps to coordinate with intelligence, law enforcement, and public agencies; establish information sharing agreements; physical protection of key assets; access controls; awareness and readiness training programs; warning and alarm systems; and practices to reduce the threat.

Organizational culture, operational plans, and management objectives should motivate individuals to feel personally responsible for prevention, avoidance, deterrence, and detection.

Deterrence and detection can make a disruptive act or activity more difficult to carry out against the organization or significantly limit, if not negate, its impact. Consideration of prevention, detection, and deterrence strategies may be:

e) Architectural: Natural or manmade barriers; redesigned or relocated infrastructure.

f) Operational: Administrative procedures, removal of hazardous materials; redesigned systems and operations; security officers' post orders; employee awareness programs; counter

surveillance and counter intelligence as avoidance; relocation of systems, operations, infrastructure, and personnel.

g) Technological: Alternative materials and processes, interoperable communication and information networks, intrusion detection, access control, recorded surveillance, package and baggage screening, and system controls.

Physical security planning includes protection of perimeter grounds, building perimeter, internal space protection, and protection of assets and contents. Defense begins at the external perimeter.

a) Physical security planning is a function of detection, deter, delay, and response.

b) Physical security measures should be designed so detection is as far from the target as possible. Delays are planned closer to the target.

c) Security system design should link exterior or interior detection with assessment and response.

d) Physical security measures may include crime prevention through environmental design; physical barriers and site hardening; physical entry and access controls; security lighting; intrusion detection systems and alarms; closed-circuit televisions; security personnel; and security policies and procedures.

Cost-effective mitigation strategies should be employed to prevent or lessen the impact of potential crises.

a) The mitigation strategy should consider immediate, interim, and long-term actions.

b) The various resources that would contribute to the mitigation process should be identified. These resources – including essential personnel and their roles and responsibilities, facilities, technology, and equipment – should be documented in the plan and become part of "business as usual."

c) Systems and resources should be monitored continually as part of mitigation strategies. Such monitoring can be likened to simple inventory management.

d) The resources that will support the organization to mitigate the crisis should also be monitored continually to ensure that they will be available and able to perform as planned during the disruption and crisis. Examples of such systems and resources include, but are not limited to: emergency equipment, fire alarms and suppression systems, local resources and vendors, alternate worksites, maps and floor plans, system backup, and offsite storage.

A.4.7.3 Response

Preparedness and response plans should be developed around a realistic "worst case scenario," with the understanding that the response can be scaled appropriately to match the actual crisis.

People are the most important aspect of any preparedness and response plan. How an organization's human resources are managed will impact the success or failure of incident management.

a) A system should be devised by which all personnel can be accounted for quickly after the onset of a crisis. This system could range from a simple telephone tree to an elaborate external vendor's call-in site. Current and accurate contact information should be maintained for all

personnel. Consideration should be given to engaging the company's travel services to assist in locating employees on business travel.

b) Arrangements should be made for notification of any next-of-kin in case of injuries or fatalities. If at all possible, notification should take place in person by a member of top management. Appropriate training should be provided.

c) The organization should implement a Family Representative program in case of severe injury or fatality. The Family Representative should be someone other than the person who performed the notification. This representative should act as the primary point of contact between the family and the organization. Comprehensive training for the representative is a necessity.

d) Crisis counseling should be arranged as necessary. In many cases, such counseling goes beyond the qualifications and experience of an organization's employee assistance program (where available). Other reliable sources of counseling should be identified prior to a crisis situation.

e) A crisis may have far reaching financial implications for the organization, its employees and their families, and other stakeholders; these implications should be considered an important part of a preparedness and response plan. Implications may include financial support to families of victims. Additionally, there may be tax implications that should be referenced and clarified in advance.

f) The payroll system should remain functional throughout the crisis.

Logistical decisions made in advance will impact the success or failure of a good preparedness and response plan. Among them are the following:

a) A primary Crisis Management Center should be identified in advance. This is the initial site used by the Crisis Management Team and Response Teams for directing and overseeing crisis management activities. The site should have an uninterruptible power supply; essential computer, telecommunications, heating/ventilating/air conditioning systems; and other support systems. Additionally, emergency supplies should be identified and kept in the center.

b) Where a dedicated center is not possible, a designated place where the teams may direct and oversee crisis management activities should be guaranteed. Access control measures should be implemented, with the members of all teams given 24x7 access.

c) A secondary Crisis Management Center should also be identified in the event that the primary center is impacted by the crisis event.

d) The organization should consider the establishment of virtual command centers for distributed access to information as well as to reach dispersed or remote stakeholders.

Once the Crisis Management Team has been activated, the damage should be assessed. The damage assessment may be performed by the Crisis Management Team itself or a designated Damage Assessment Team. Responsibility should be assigned for the documentation of all incident related facts and response actions, including financial expenditures.

a) For situations involving physical damage to company property, the Crisis Management Team or its designated Damage Assessment Team should be mobilized to the site. The team will gain entry if permission from the public safety authorities is granted, and make a preliminary

assessment of the extent of damage and the likely length of time that the facility will be unusable.

b) Certain types of disruptions do not involve immediate physical damage to a company worksite or facility. These would include the business, human, information technology, and societal types of crises. In these crises, the team will likely assess the damage or impact as the disruption unfolds.

If appropriate, existing funding and insurance policies should be examined, and additional funding and insurance coverage should be identified and obtained.

a) Policy parameters should be established in advance, including pre-approval by the insurance provider of any response related vendors. Where possible, the amount of funds to help ensure continuity of operations should be determined in the planning process.

b) Any cash should be stored in an easily accessible location to assure its availability during a crisis, and some cash and credit should be available for weekend and after-hours requirements.

c) All disruption and crisis related expenses should be recorded throughout the response and recovery periods.

d) Insurance providers should be contacted as early as possible in the response period, particularly in instances of a wide-reaching crisis, where competition for such resources could be vigorous. All insurance policy and contact information should be readily available to the Crisis Management Team and backed up or stored offsite as appropriate.

Transportation in a time of a disruption or crisis can be a challenge. Provisions should be arranged ahead of time, if possible. Areas where transportation is critical include, but are not limited to:

a) Evacuation of personnel (this may be from a demolished work-site or from a satellite facility in another region or country);

b) Transportation to an alternate worksite;

c) Supplies into the site or to an alternate site;

d) Transportation of critical data to worksite; and

e) Transportation for staff with special needs.

A.4.7.4 Continuity and Recovery Plans

The organization should establish documented procedures that detail how the organization will manage a disruptive event and how it will recover or maintain its activities to a predetermined level, based on management-approved recovery objectives.

a) Supply chain, critical vendor or service provider agreements should be established as appropriate and their contact information maintained as part of the preparedness, response, continuity and recovery plans. Such information could include phone numbers, contact names, account numbers, pass-codes (appropriately protected), and other information in the event that someone unfamiliar with the process would need to make contact.

b) In to avoid disruption of the supply chain, it may be appropriate to request and review the preparedness, response, continuity and recovery plans of supply chain partners and critical vendors, in order to evaluate their ability to continue to provide necessary supplies and services in the case of a far-reaching crisis. At a minimum, the supply chain, vendor, or service provider roles and service level agreements should be discussed in advance of the crisis.

c) The organization should have alternate worksites identified for business resumption and recovery. In the absence of other company facilities being available and/or suitable, access to alternate worksites can be arranged through appropriate vendors. Planning concerning the identification and availability of alternate worksites should take place early in the preparedness and response plan process. Alternate worksites should provide adequate access to the resources required for business resumption identified in the impact analysis.

d) Offsite storage of data and assets is a valuable mitigation strategy allowing rapid crisis response and business resumption/recovery. The off-site storage location should be a sufficient distance from the primary facility so that it is not likely to be similarly affected by the same event. Items to be considered for off-site storage include critical and vital records (paper and other media) critical to the operations of the business. Procedures should be included in the plan to ensure the timely delivery of any necessary items from offsite storage to the Crisis Management Center or the alternate worksites.

e) Mutual aid agreements identify resources that may be shared with or borrowed from other organizations during a disruption, as well as mutual support that may be shared with other organizations. Such agreements should be legally sound and properly documented, clearly understood by all parties involved, and representative of dependable resources as well as a commitment to cooperation.

f) Strategic alliances identify delivery partners with which it has an interdependent relationship with other organizations to produce and supply products and services and share risk.

g) Once the extent of damage is known, the process recovery needs should be prioritized and a schedule for resumption determined and documented. The prioritization should take into account the fundamental criticality of the process and other factors, including relationships to supply chain obligations, other processes, critical schedules, and regulatory requirements, as identified in the criticality and impact analysis. Decisions regarding prioritization of processes should be documented and recorded, including the date, time, and justification for the decisions.

h) Once the processes to be restored have been prioritized, the resumption work can begin with processes restored according to the prioritization schedule. The resumption of these processes may occur at either the current worksite or an alternate worksite, depending on the circumstances of the crisis. Documentation should be kept of when the processes were resumed.

i) Once the critical processes have been resumed, the resumption of the remaining processes can be addressed. Where possible, decisions about the prioritization of these processes should be thoroughly documented in advance, as should the timing of actual resumption.

j) The organization should seek to bring the organization "back to normal." If it is not possible to return to the pre-crisis "normal," a "new normal" should be established. This "new normal" creates the expectation that, while there may be changes and restructuring in the workplace, the

organization will phase back into productive work. Each step of the process and all decisions should be carefully documented.

k) As a rule, it is at this point that the crisis may be officially declared "over." It is important to document this decision. Press conferences and mass media communications may be undertaken to bolster employee and client confidence.

A.5 Checking and Corrective Action

A.5.1 Monitoring and Measurement

Data collected from monitoring and measurement can be analyzed to identify patterns and obtain information. Knowledge gained from this information can be used to implement corrective and preventive action. Metrics should be established to measure success of the resilience management system.

Key characteristics are those that the organization needs to consider to determine how it is managing its significant risks and impacts, achieving objectives and targets, and improving security, preparedness, response, continuity, and recovery performance.

When necessary to ensure valid results, measuring equipment should be calibrated or verified at specified intervals, or prior to use, against measurement standards traceable to international or national measurement standards. Where no such standards exist, the basis used for calibration should be recorded.

A.5.2 Evaluation of Compliance and System Performance

A.5.2.1 Evaluation of Compliance

The organization should be able to demonstrate that it has evaluated compliance with the legal requirements identified including applicable permits or licenses.

The organization should be able to demonstrate that it has evaluated compliance with the identified other requirements to which it has subscribed.

A.5.2.2 Exercises and Testing

Testing scenarios should be designed using the events identified in the risk assessment and impact analysis.

Testing can keep response teams and employees effective in their duties, clarify their roles, and reveal weaknesses in the resilience management system that should be corrected. A commitment to testing lends credibility and authority to the resilience management system.

The first step in testing should be the setting of goals and expectations. A critical goal is to determine whether a certain disruption response process works and how it can be improved. Other examples of goals include:

a) Capacity testing (e.g., the capacity of a call-in or call-out phone system);

b) Reduce the time necessary for accomplishment of a process (e.g., using repeated drills to shorten response times); and

c) Bring awareness and knowledge to the general employee population about the resilience management system.

Lessons learned from previous tests, as well as actual incidents experienced, should be built into the testing cycle for the resilience management system.

The responsibility for testing the resilience management system should be assigned. Larger organizations may consider establishing a Test Team. Where appropriate, the expertise of external resources (consultants, local emergency organizations, etc.) can be leveraged.

A test schedule and timeline as to how often the plan and its components will be tested should be established.

The scope of testing should be planned to develop over time. Tests should start out relatively simple, becoming increasingly complex as the test process evolves. Early tests may include checklists, simple exercises, and small components of the resilience management system. As the test schedules evolve, tests should become increasingly complex, up to a full-scale activation of the entire resilience management system, including external participation by public safety and emergency responders.

There are several roles that test participants can fill. All participants should understand their roles in the exercise, and the exercise should involve all participants. Various groups from the organization itself, as well as from the public sector, can participate in the tests. As part of the exercise, participants should be allowed to interact and discuss issues and lessons.

After completion, the exercises and tests should be critically evaluated. The evaluation should include, among other things, an assessment of how well the goals and objectives of the test were achieved, the effectiveness of participation, and whether the resilience management system itself will function as anticipated in the case of a real crisis. Future testing, as well as the resilience management system itself, should then be modified as necessary based on the test results.

Design of tests should be evaluated and modified as necessary. They should be dynamic, taking into account changes to the resilience management system, personnel turnover, actual incidents, and results from previous exercises.

Exercise and test results should be documented.

A.5.3 Nonconformity, Corrective Action, and Preventive Action

Depending on the nature of the nonconformity, in establishing procedures to deal with these requirements, organizations may be able to accomplish them with a minimum of formal planning, or it may be a more complex and long-term activity. Any documentation should be appropriate to the level of action.

A.5.4 Control of Records

Management system records can include, among others:

a) Compliance records;
b) Training records;
c) Process monitoring records;
d) Inspection, maintenance, and calibration records;
e) Pertinent contractor and supplier records;
f) Incident reports;
g) Records of incident and emergency preparedness tests;
h) Audit results;
i) Management review results;
j) External communications decision;
k) Records of applicable legal requirements;
l) Records of significant risk and impacts;
m) Records of management systems meetings;
n) Security, preparedness, response, continuity, and recovery performance information;
o) Legal compliance records; and
p) Communications with stakeholders and interested parties.

Proper account should be taken of confidential information.

Organizations should ensure the integrity of records by rendering them tamperproof, securely backed-up, accessible only to authorized personnel, and protected from damage, deterioration, or loss.

The organization should consult with the appropriate legal authority within their organization to determine the appropriate period of time the documents should be retained and establish, implement, and maintain the processes to effectively do so.

NOTE: Records are not the sole source of evidence to demonstrate conformity to this *Standard*.

A.5.5 Internal Audit

Internal audits of a resilience management system can be performed by personnel from within the organization or by external persons selected by the organization, working on its behalf. In either case, the persons conducting the audit should be competent and in a position to do so impartially and objectively. In smaller organizations, auditor independence can be demonstrated by an auditor being free from responsibility for the activity being audited.

NOTE: If an organization wishes to combine audits of its resilience management system with security, safety, or environmental audits, the intent and scope of each should be clearly defined.

A.6 Management Review

The management review should cover the scope of the resilience management system, although not all elements of the resilience management system need to be reviewed at once and the review process may take place over a period of time.

The resilience management system should be regularly reviewed and evaluated. Reviews should occur according to a pre-determined schedule, and documentation of the review should be maintained as necessary. The following factors can trigger a review and should otherwise be examined once a review is scheduled:

a) *Risk assessment and impact analysis*: The resilience management system should be reviewed every time a risk assessment is completed for the organization. The results of the risk assessment and impact analysis can be used to determine whether the Resilience management system continues to adequately address the risks facing the organization.
b) *Sector/industry trends*: Major sector/industry initiatives should initiate a resilience management system review. General trends in the sector/industry and in business/operational continuity planning techniques can be used for benchmarking purposes.
c) *Regulatory requirements*: New regulatory requirements may require a review of the Resilience management system.
d) *Event experience*: A review should be performed following a response to disruptive incident, whether the response plan was activated or not. If the plan was activated, the review should take into account the history of the plan itself, how it worked, why it was activated, etc. If the plan was not activated, the review should examine why and whether this was an appropriate decision.
e) *Test and exercise results*: Based on test and exercise results, the Resilience management system should be modified as necessary.

Continual improvement and resilience management system maintenance should reflect changes in the risks, activities, functions, and operation of the organization that will affect the resilience management system. The following are examples of procedures, systems, or processes that may affect the plan:

a) Policy changes;
b) Hazards and threat changes;
c) Changes to the organization and its business processes;
d) Changes in supply chain flows, nodes and obligations;
e) Changes in assumptions in risk assessment and impact analysis;
f) Personnel changes (employees and contractors);
g) Supplier and supply chain changes;
h) Process and technology changes;
i) Systems and application software changes;
j) Critical lessons learned from testing;
k) Issues discovered during actual implementation of the plan in a crisis;

l) Changes to external environment (new businesses in area, new roads or changes to existing traffic patterns, etc.); and

m) Other items noted during review of the plan and identified during the risk assessment and impact analysis.

Annex B
(informative)

B COMPATIBILITY WITH OTHER MANAGEMENT SYSTEMS

This *Standard* is aligned with ISO 9001:2000, ISO 14001:2004, ISO/IEC 27001:2005, and ISO 28000:2007 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards.

The integrated approach can help avoid segregating or "siloing" risks, and provides an overall risk profile allowing the organization to better understand the relationships between risks and identify solutions to problems. It leverages the perspectives, knowledge, and capabilities of divisions and individuals within an organization. Because of the relatively low probability and yet potentially high consequence nature of many natural, intentional, or unintentional threats and hazards that an organization may face, an integrated approach allows an organization to establish priorities that address its individual needs for risk management within an economically sound context.

For example, this *Standard* may be applied in parallel to or integrated with ISO 14001:2004, *Environmental management systems – Requirements with guidance for use.* The management approach contains all the elements required for implementation of the ISO 14001:2004. In order to conduct a parallel or integrated application, the risk assessment and impact analysis should include consideration of:

- *Environmental aspects*: Elements of an organization's activities or products or services that can interact with the environment. A significant environmental aspect has or can have a significant environmental impact.
- *Environmental impact*: Any change to the environment, whether adverse or beneficial, wholly or partially resulting from an organization's environmental aspects.

Reduction, removal, and management of an organization's hazardous materials will provide proactive benefits from both the environmental and security perspectives by providing protection from and response to risks of unintentionally, intentionally, and naturally-caused events.

Table 1: Correspondence between ISO 9001:2000, ISO 14001:2004, ISO 27001:2005, and this *Standard* of Best Practices

Resilience in the Supply Chain Management System Standard	ISO 9001:2000	ISO 14001:2004	ISO 27001:2005
0 Introduction 0.1 General 0.2 Process approach 0.3 Qualifications 0.4 Process approach Annex B: Compatibility with other management systems	0 Introduction 0.1 General 0.2 Process approach 0.3 Relationship with ISO 9004 0.4 Compatibility with other management systems	Introduction	0 Introduction 0.1 General 0.2 Process approach 0.3 Compatibility with other management systems
1 Scope	1 Scope 1.1 General 1.2 Application		1 Scope 1.1 General 1.2 Application
2 Normative references	**2 Normative reference**	**2 Normative reference**	**2 Normative references**
3 Terms and definitions	**3 Terms and definitions**	**3 Terms and definitions**	**3 Terms and definitions**
4 Organizational Resilience (OR) management system 4.1 General requirements 4.1.1 Understanding the Organization and its Context 4.1.2 Scope of Resilience Management System 4.1.3 Provision of Resources for the Resilience Management System 4.2 Resilience management policy 4.2.1 Policy statement 4.2.2 Management commitment	**4 Quality management system** 4.1 General requirements 5 Management responsibility 5.1 Management commitment 5.2 Customer focus 5.3 Quality policy 5.4 Planning 5.5 Responsibility, authority and communication	**4 Environmental management system requirements** 4.1 General requirements 4.2 Environmental policy	**4 Information security management system (ISMS)** 4.1 General requirements 4.2 Establishing and managing the ISMS 4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS 4.2.4 Maintain and improve the ISMS 5 Management responsibility 5.1 Management commitment
4.3 Planning 4.3.1 Risk Assessment and Monitoring 4.3.1.1 Internal and External Communication and Consultation 4.3.1.2 Monitoring and Reviewing the Risk Assessment Process 4.3.2 Legal and other requirements 4.3.3 Resilience Objectives and Targets 4.3.4 Strategic Plans and Programs for Resilience	**7 Product realization** 7.1 Planning of product realization 7.2 Customer-related processes 7.2.1 Determination of requirements related to the product 7.2.2 Review of requirements related to the product	**4.3 Planning** 4.3.1 Environmental aspects 4.3.2 Legal and other requirements 4.3.3 Objectives, targets and program(s)	**4.2 Establishing and managing the ISMS** 4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS

Resilience in the Supply Chain Management System Standard	ISO 9001:2000	ISO 14001:2004	ISO 27001:2005
4.4 Implementation and operation 4.4.1 Resources, Roles, Responsibility, and Authority for Resilience Management 4.4.2 Competence, Training, and Awareness 4.4.3 Communication and Warning 4.4.4 Documentation 4.4.5 Control of Documents 4.4.6 Operational Control 4.4.7 Incident Prevention, Preparedness, and Response 4.4.7.1 Prevention, Preparedness, and Response Structure 4.4.7.2 Prevention, Protection and Mitigation 4.4.7.3 Response 4.4.7.4 Continuity and Recovery Plans	**6 Resource management** 6.1 Provision of resources 6.2 Human resources 6.2.2 Competence, awareness and training 6.3 Infrastructure 6.4 Work environment 7.2.3 Customer communication 4.2 Documentation requirements 4.2.1 General 4.2.2 Quality manual 4.2.3 Control of documents 7.3 Design and development 7.4 Purchasing 7.5 Product and service provision	**4.4 Implementation and operation** 4.4.1 Resources, roles, responsibility and authority 4.4.2 Competence, training, and awareness 4.4.3 Communication and warning 4.4.4 Documentation 4.4.5 Control of documents 4.4.6 Operational control 4.4.7 Emergency preparedness and response	**5.2 Resource management** 5.2.1 Provision of resources 5.2.2 Training, awareness and competence 4.3 Documentation requirements 4.3.1 General 4.3.2 Control of documents
4.5 Checking 4.5.1 Monitoring and Measurement 4.5.2 Evaluation of Compliance and System Performance 4.5.2.1 Evaluation of Compliance 4.5.2.2 Exercises and Testing 4.5.3 Nonconformity, Corrective Action, and Preventive Action 4.5.4 Control of Records 4.5.5 Internal Audits	7.6 Control of monitoring and measuring devices 8.2.3 Monitoring and measurement of processes 8.2.4 Monitoring and measurement of product 8.3 Control of nonconforming product 8.5.3 Corrective actions 8.5.3 Preventive actions 4.2.4 Control of records 8.2.2 Internal Audit 8.4 Analysis of data	**4.5 Checking** 4.5.1 Monitoring and measurement 4.5.2 Evaluation of compliance 4.5.3 Nonconformity, corrective action and preventive action 4.5.4 Control of records 4.5.5 Internal audits	4.2.3 Monitor and review the ISMS 8.2 Corrective action 8.3 Preventive action 4.3.3 Control of records 6 Internal ISMS audits
4.6 Management review 4.6.1 General 4.6.2 Review Input 4.6.3 Review Output 4.6.4 Maintenance 4.6.5 Continual Improvement	**5.6 Management review** 5.6.1 General 5.6.2 Review input 5.6.3 Review output 8.5 Improvement 8.5.1 Continual improvement	**4.6 Management review**	**7 Management review of the ISMS** 7.1 General 7.2 Review input 7.3 Review output 4.2.4 Maintain and improve 8 ISMS improvement 8.1 Continual improvement he ISMS
Annex A Control objectives and controls **Annex B Correspondence between ISO 9001:2000, ISO 14001:2004, ISO 27001:2005 and this *Standard* of Best Practices**	**Annex A Correspondence between ISO 9001:2000 and ISO 14001:1996**	**Annex A Guidance on the use of this International Standard** **Annex B Correspondence between ISO 14001:2004 and ISO 9001:2000**	**Annex A Control objectives and controls** **Annex B OECD principles and this International Standard** **Annex C Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard**

Annex C
(informative)

C TERMINOLOGY CONVENTIONS

The terminology conventions in Table 2 are in accordance with ISO/IEC – Directives Part 2: *Rules for the structure and drafting on International Standards, Annex H, Verbal forms for the expression of provisions*, 2004.

Table 2: Verbal forms for the expression of provisions

Verbal form	Usage (ISO/IEC – Directives Part 2: ***Rules for the structure and drafting on International Standards***)
shall	Auditable requirements of a document – "used to indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted."
should	Recommendations – "used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited."
may	Permission – "used to indicate a course of action permissible within the limits of the document."
can	Possibility and capability – "used for statements of possibility and capability, whether material, physical or causal."

Items presented in lists shall not be construed to be exhaustive, unless otherwise stated. Nor shall the order of the list be viewed as specifying a sequence or priority, unless so stated. The generic nature of this *Standard* allows for organization to include additional items as well as designation of a sequence or priority based on the specific operating conditions and circumstances of the organization.

Annex D
(normative)

D GLOSSARY

For the purposes of this document, the terms and definitions given in ISO/IEC Guide 73 and the following definitions apply.

D.1 acceptable downtime: Maximum elapsed time between a disruption and restoration of needed operational capacity or capability.

D.2 alternate worksite: A work location, other than the primary location, to be used when the primary location is not accessible. [ASIS International Business Continuity Guideline: 2005]

D.3 asset: Anything that has value to the organization. [ISO/IEC 13335-1:2004]

D.4 auditor: Person with competence to conduct an audit. [ISO 9001:2000]

D.5 continual improvement: Recurring process of enhancing the organizational resilience (OR) management system in order to achieve improvements in overall Resilience management performance consistent with the organization's Resilience management policy.

NOTE: The process need not take place in all areas of activity simultaneously.

D.6 corrective action: Action to eliminate the cause of a detected nonconformity. [ISO 14001:2004]

D.7 critical activity: Any function or process that is essential for the organization to deliver its products and/or services. [ISO/PAS 22399:2007]

D.8 criticality assessment: A process designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a disruption on the continuity of the organization.

D.9 conformity: Fulfillment of a requirement.

D.10 consequence: Outcome of an event. [ISO/IEC Guide 73]

NOTE 1: There can be more than one consequence from one event.

NOTE 2: Consequences can range from positive to negative.

NOTE 3: Consequences can be expressed qualitatively or quantitatively.

D.11 continuity: Strategic and tactical capability, pre-approved by management, of an organization to plan for and respond to conditions, situations, and events in order to continue operations at an acceptable predefined level.

NOTE: *Continuity*, as used in this *Standard*, is the more general term for operational and business continuity to ensure an organization's ability to continue operating outside of normal operating conditions. It applies not only to for-profit companies, but organizations of all natures, such as non-governmental, public interest, and governmental organizations.

D.12 continuity strategy: Approach by an organization intended to ensure continuity and ability to recover in the face of a disruptive event, emergency, crisis, or other major outage.

D.13 crisis: An unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.

D.14 crisis management: Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective

response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities – as well as effectively restoring operational capabilities.

NOTE: Crisis management also involves the management of preparedness, mitigation response, and continuity or recovery in the event of an incident – as well as management of the overall program through training, rehearsals, and reviews to ensure the preparedness, response, and continuity plans stays current and up-to-date.

D.15 crisis management team: Group of individuals functionally responsible for directing the development and execution of the response and operational continuity plan, declaring an operational disruption or emergency/crisis situation, and providing direction during the recovery process, both pre-and post-disruptive incident.

NOTE: The crisis management team may include individuals from the organization as well as immediate and first responders, stakeholders, and other interested parties.

D.16 criticality: Of essential importance with respect to objectives and/or outcomes.

D.17 damaging potential: Harmful potential of an event, whether anticipated or unanticipated, that would impact on the ability of the organization to function effectively, cause critical harm to infrastructure, result in significant human resilience property losses to the organization or its stakeholders, or cause adverse effects to the reputation or integrity of the organization.

D.18 disaster: Event that causes great damage or loss. [ISO/PAS 22399:2007]

D.19 disruption: An event that interrupts normal business, functions, operations, or processes, whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a blackout, terror attack, technology failure, or earthquake).

NOTE: A disruption can be caused by either positive or negative factors that will disrupt normal functions, operations, or processes.

D.20 document: Information and supporting medium. [ISO 9000:2000]

NOTE: The medium can be paper, magnetic, electronic or optical computer disc, photography or master sample, or a combination thereof.

D.21 emergency: Sudden, urgent, usually unexpected occurrence or event requiring immediate action. [ISO/PAS 22399:2007]

NOTE: An emergency is usually a disruptive event or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

D.22 exercises: Evaluating Resilience management programs, rehearsing the roles of team members and staff, and testing the recovery or continuity of an organization's systems (e.g., technology, telephony, administration) to demonstrate Resilience management competence and capability.

NOTE 1: Exercises include activities performed for the purpose of training and conditioning team members and personnel in appropriate responses with the goal of achieving maximum performance.

NOTE 2: An exercise can involve invoking response and operational continuity procedures, but is more likely to involve the simulation of an response and/or operational continuity incident, announced or unannounced, in which participants role-play in order to assess what issues might arise, prior to a real invocation.

D.23 evacuation: Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas. [ASIS International Business Continuity Guideline: 2005]

D.24 event: Occurrence or change of a particular set of circumstances. [ISO/IEC Guide 73]

NOTE 1: Nature, likelihood, and consequence of an event can not be fully knowable.

NOTE 2: An event can be one or more occurrences, and can have several causes.

NOTE 3: Likelihood associated with the event can be determined.

NOTE 4: An event can consist of a non occurrence of one or more circumstances.

NOTE 5: An event with a consequence is sometimes referred to as "incident".

D.25 facility (infrastructure): Plant, machinery, equipment, property, buildings, vehicles, information systems, transportation facilities, and other items of infrastructure or plant and related systems that have a distinct and quantifiable function or service.

D.26 hazard: Possible source of danger, or conditions (physical or operational) that have a capacity to produce a particular type of adverse effects. [ISO/PAS 22399:2007]

D.27 impact: Evaluated consequence of a particular outcome. [ISO/PAS 22399:2007]

D.28 impact analysis: Process of analyzing all operational functions and the effect that an operational interruption might have upon them.

NOTE: Impact analysis includes *Business Impact Analysis* – the identification of critical business assets, functions, processes, and resources as well as an evaluation of the potential damage or loss that may be caused to the organization resulting from a disruption (or a change in the business or operating environment). Impact analysis identifies: 1) how the loss or damage will manifest itself; 2) how that degree for potential escalation of damage or loss with time following an Incident; 3) the minimum services and resources (human, physical, and financial) needed to enable business processes to continue to operate at a minimum acceptable level; and 4) the timeframe and extent within which activities, functions, and services of the organization should be recovered.

D.29 incident: Event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis, or disaster.

D.30 integrity: The property of safeguarding the accuracy and completeness of assets. [ISO/IEC 13335-1:2004]

D.31 internal audit: Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the management system audit criteria set by the organization are fulfilled.

NOTE: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.

D.32 management plan: Clearly defined and documented plan of action, typically covering the key personnel, resources, services, and actions needed to implement the incident management process.

D.33 mitigation: Limitation of any negative consequence of a particular incident. [ISO/PAS 22399:2007]

D.34 mutual aid agreement: Pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement. [ISO/PAS 22399:2007]

D.35 nonconformity: Non-fulfillment of a requirement. [ISO 9000:2000]

D.36 objective: Overall goal, consistent with the policy that an organization sets itself to achieve. [ISO 14001:2004]

D.37 organization: Group of people and facilities with an arrangement of responsibilities, authorities, and relationships. [ISO/PAS 22399:2007]

NOTE: An organization can be a government or public entity, company, corporation, firm, enterprise, institution, charity, sole trade or association, or parts or combinations thereof.

D.38 policy: Overall intentions and direction of an organization, as formally expressed by top management.

D.39 preparedness (readiness): Activities, programs, and systems developed and implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions, disasters, or emergencies.

D.40 prevention: Measures that enable an organization to avoid, preclude, or limit the likelihood or impact of a disruption.

D.41 preventive action: Action to eliminate the cause of a potential nonconformity. [ISO 14001:2004]

D.42 prevention of hazards and threats: Process, practices, techniques, materials, products, services, or resources used to avoid, reduce, or control hazards and threats and their associated risks of any type in order to reduce their potential impact.

D.43 probability: Extent to which an event is likely to occur. [ISO/IEC Guide 73]

NOTE 1: ISO 3534-1:1993, Definition 1.1, gives the mathematical definition of probability as "a real number in the scale of 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1."

NOTE 2: Frequency rather than probability may be used to describe risk.

NOTE 3: Degrees of belief about probability can be chosen as classes or ranks, such as:

- rare/unlikely/moderate/likely/almost certain; or
- incredible/improbable/remote/occasional/probable/frequent.

D.44 procedure: Specified way to carry out an activity. [ISO 9000:2000]

NOTE: Procedures can be documented or not.

D.45 record: Document stating results achieved or providing evidence of activities performed. [ISO 9000:2000]

D.46 recovery time objective (RTO): Time goal for the restoration and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations.

D.47 residual risk : Risk remaining after risk treatment. [ISO/PAS 22399:2007]

D.48 resilience: The adaptive capacity of an organization in a complex and changing environment.

NOTE 1: Resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.

NOTE 2: Resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must.

D.49 organizational resilience (OR) management: Systematic and coordinated activities and practices through which an organization manages its operational risks, and the associated potential threats and impacts therein.

D.50 organizational resilience (OR) management program: Ongoing management and governance process supported by top management; resourced to ensure that the necessary steps are taken to identify the root causes of potential disruptions, likelihood and impact of potential losses; maintain viable adaptive, proactive and reactive strategies and plans; and ensure stability and sustainability of activities/functions/products/services through planning, exercising, rehearsal, testing, training, maintenance, and assurance.

D.51 resources: Any asset (human, physical, information or intangible), facilities, equipment, materials, products or waste that has potential value and can be used.

D.52 response plan: Documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident.

D.53 response program: Plan, processes, and resources to perform the activities and services necessary to preserve and protect life, property, operations, and critical assets. [ISO/PAS 22399:2007]

NOTE: Response steps generally include incident recognition, notification, assessment, declaration, plan execution, communications, and resources management

D.54 response team: Group of individuals responsible for developing, executing, rehearsing, and maintaining the response plan, including the processes and procedures.

D.55 risk: Effect of uncertainty on objectives. [ISO/IEC Guide 73]

NOTE 1: An effect is a deviation from the expected – positive and/or negative.

NOTE 2: Objectives can have different aspects such as financial, health and safety, and environmental goals and can apply at different levels such as strategic, organization-wide, project, product, and process.

NOTE 3: Risk is often characterized by reference to potential events, consequences, or a combination of these and how they can affect the achievement of objectives.

NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances, and the associated likelihood of occurrence.

D.56 risk acceptance: Informed decision to take a particular risk. [ISO/IEC Guide 73]

NOTE 1: Risk acceptance can occur without risk treatment or during the process of risk treatment.

NOTE 2: Risk acceptance can also be a process.

NOTE 3: Risks accepted are subject to monitoring and review.

D.57 risk analysis: Process to comprehend the nature of risk and to determine the level of risk. [ISO/IEC Guide 73]

NOTE: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

D.58 risk assessment: Overall process of risk identification, risk analysis, and risk evaluation.

NOTE: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the probability and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

D.59 risk communication: Exchange or sharing of information about risk between the decision-maker and other stakeholders. [ISO/IEC Guide 73]

NOTE: The information can relate to the existence, nature, form, probability, severity, acceptability, treatment, or other aspects of risk.

D.60 risk criteria: Terms of reference by which the significance of risk is assessed. [ISO/IEC Guide 73]

NOTE: Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of stakeholders, priorities, and other inputs to the assessment.

D.61 risk management: Coordinated activities to direct and control an organization with regard to risk. [ISO/IEC Guide 73]

NOTE: Risk management generally includes risk assessment, risk treatment, risk acceptance, and risk communication.

D.62 risk reduction: Actions taken to lessen the probability, negative consequences, or both, associated with a risk. [ISO/IEC Guide 73]

D.63 risk tolerance: Organization's readiness to bear the risk after risk treatments in order to achieve its objectives. [ISO/IEC Guide 73]

NOTE Risk tolerance can be limited by legal or regulatory requirements.

D.64 risk transfer: Sharing with another party the burden of loss or benefit or gain, for a risk. [ISO/IEC Guide 73]

NOTE 1: Legal or statutory requirements can limit, prohibit ,or mandate the transfer of certain risk.

NOTE 2: Risk transfer can be carried out through insurance or other agreements.

NOTE 3: Risk transfer can create new risks or modify existing risks.

NOTE 4: Relocation of the source is not risk transfer.

D.65 risk treatment: Process of selection and implementation of measures to modify risk. [ISO/IEC Guide 73]

NOTE 1: The term "risk treatment" is sometimes used for the measures themselves.

NOTE 2: Risk treatment measures can include avoiding, optimizing, transferring, or retaining risk.

D.66 security: The condition of being protected against hazards, threats, risks, or loss.

NOTE 1: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside.

NOTE 2: The term "security" means that something not only is secure but that it has been secured.

D.67 security aspects: Those characteristics, elements, or properties which reduce the risk of unintentionally, intentionally, and naturally-caused crises and disasters that disrupt and have consequences on the products and services, operation, critical assets, and continuity of the organization and its stakeholders.

D.68 simulation exercise: Test performed under conditions as close as practicable to real world conditions. [ISO/PAS 22399:2007]

D.69 source: Anything which alone or in combination has the intrinsic potential to give rise to risk. [ISO/IEC Guide 73]

NOTE: A risk source can be tangible or intangible.

D.70 stakeholder (interested party): Person or group having an interest in the performance or success of an organization.

NOTE: The term includes persons and groups with an interest in an organization, its activities and its achievements – e.g., customers, clients, partners, employees, shareholders, owners, vendors, the local community, first responders, government agencies, and regulators.

D.71 supply chain: The linked set of resources and processes that begins with the acquisition of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include suppliers, vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and other entities that lead to the end user.

D.72 target: Detailed performance requirement applicable to the organization (or parts thereof) that arises from the objectives and that needs to be set and met in order to achieve those objectives. [ISO 14001:2004]

D.73 testing: Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties, and to reveal weaknesses in the preparedness and response/continuity/recovery plans. [ASIS International Business Continuity Guideline: 2005]

D.74 threat: Potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community.

D.75 top management: Directors, managers, and officers of an organization that can ensure effective management systems – including financial monitoring and control systems – have been put in place to protect assets, earning capacity, and the reputation of the organization.

D.76 vulnerability: Intrinsic properties of something that create susceptibility to a source of risk (D.53) that can lead to a consequence. [ISO/IEC Guide 73]

D.77 vulnerability assessment: The process of identifying and quantifying vulnerabilities.

Annex E
(informative)

E QUALIFICATIONS

The adoption and implementation of a range of security, preparedness, and continuity management techniques in a systematic manner can contribute to optimal outcomes for all stakeholders and affected parties. However, adoption of this *Standard* will not by itself guarantee optimal security, preparedness, continuity, and response outcomes. In order to achieve its objectives, the Resilience management system should incorporate the best available practices, techniques, and technologies, where appropriate and where economically viable. The cost-effectiveness of such practices, techniques, and technologies should be taken fully into account.

This *Standard* does not establish absolute requirements for security, preparedness, response, continuity, or recovery performance beyond commitments in the organization's policy to:

a) Comply with applicable legal requirements and with other requirements to which the organization subscribes;
b) Support critical risk prevention and minimization; and
c) Promote continual improvement.

The main body of this *Standard* contains only those generic criteria that may be objectively audited. Guidance on supporting Resilience management techniques is contained in the other annexes of this document.

This *Standard*, like other management standards, is not intended to be used to create non-tariff trade barriers or to increase or change an organization's legal obligations. Indeed, compliance with a standard does not in itself confer immunity from legal obligations. For organizations that so wish, an external or internal auditing process may verify compliance of their Resilience management system to this *Standard*. Verification may be by an acceptable first-, second-, or third-party mechanism. Verification does not require third-party certification.

This *Standard* does not include requirements specific to other management systems such as those for quality, occupational health and safety, or financial risk management – though its elements can be aligned or integrated with those of other management systems. It is possible for an organization to adapt its existing management system(s) in order to establish a resilience management system that conforms to the criteria of this *Standard*. It should be understood, however, that the application of various elements of the management system might differ depending on the intended purpose and the stakeholders involved.

The level of detail and complexity of the Resilience management system, the extent of documentation, and the resources devoted to it will be dependent on a number of factors – such as the scope of the system; the size of an organization; and the nature of its activities, products, and services. This may be the case in particular for small and medium-sized enterprises.

This *Standard* provides a common set of criteria for security management, preparedness, emergency management, disaster management, crisis management, and business continuity management programs. Terminology used in this standard emphasizes commonality of concepts, while acknowledging nuances in term usage in the various disciplines. For example, risk assessment includes analysis of risk, vulnerability, criticality, and impacts (consequences); however, some disciplines emphasize impact analysis. Therefore, in this document, the overall process is referred to as "risk assessment and impact analysis".

Annex F
(informative)

F BIBLIOGRAPHY

F.1 ASIS Publications

NOTE: The document below is available from ASIS. < http://www.asisonline.org/guidelines/ >

Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, 2005.

F.2 ISO Standards Publications

NOTE: All documents below are available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

[1] ISO 9001:2000*, Quality management systems — Requirements.*

[2] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use.*

[3] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management.*

[4] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing.*

[5] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements.*

[6] ISO 28000:2007, *Specification for security management systems for the supply chain.*

[7] ISO/PAS 22399:2007 *Societal Security – Guidelines for incident preparedness and operational continuity management.*

[8] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards.*