INTERNATIONAL STANDARD

ISO 28002

First edition
2011-08-01

Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use

Systèmes de management de la sécurité pour la chaîne d'approvisionnement — Développement de la résilience dans la chaîne d'approvisionnement — Exigences avec mode d'emploi

Reference number
ISO 28002:2011(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

ISO 28002 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.

This first edition cancels and replaces ISO/PAS 28002:2010.

Introduction

0.1 General

Organizations across the globe are rapidly developing risk management and resilience programs to address uncertainty in achieving their objectives. There is a strong demand for standards and best practices, as organizations 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 a 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.

During a supply chain disruption it must be emphasized that the exact nature of the disruption will probably not be fully understood at first and may only become fully understood over time. As a result resilience plans and policies developed should stress adaptation and continual evaluation of new information to ensure actions being taken are appropriate. Supply chain disruptions of sufficient magnitude will most likely attract the news media. Failure to properly manage news media relations can negatively impact resiliency response operations, resulting in a loss of stakeholder confidence. This loss of confidence can result in loss of customers, increased demand for information by government or financial organizations, and restrictions imposed by external organizations. This International 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). When implemented within a management system 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 International Standard provides generic auditable criteria to establish, check, maintain, and improve resilience policy when implemented in a management system to enhance prevention, preparedness (readiness), mitigation, response, continuity, and recovery from disruptive incidents.

This International Standard is designed to be integral to ISO 28000. It also might possibly be integrated into other management systems within an organization that follow the Plan-Do-Check-Act model. If third-party independent certification is chosen, the certification will be applied to the overall management system standard that incorporates this International Standard.

The integrated adaptive, proactive, and reactive resilience approach can leverage 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 chain 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 resilience policy. With this understanding, an organization will define to which level or tier in their supply chain to include their resilience program.

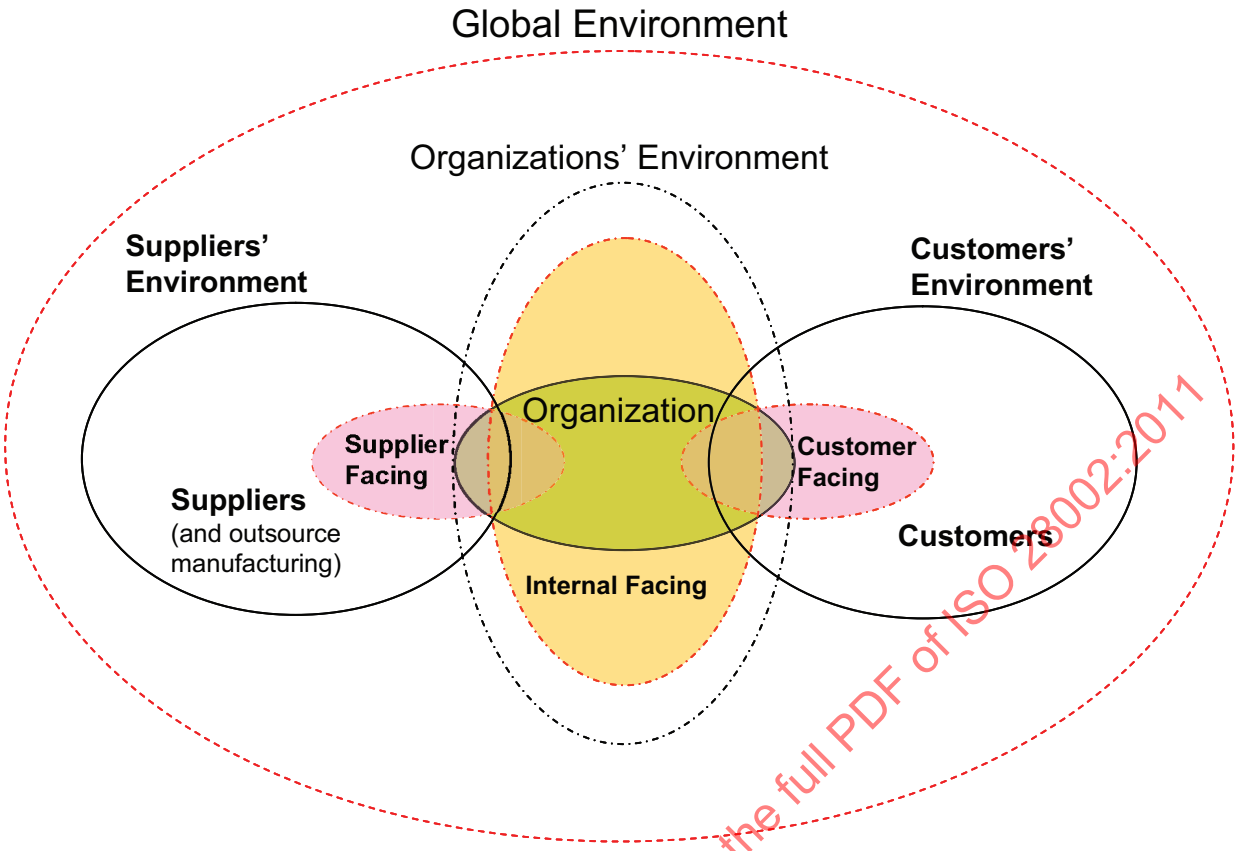

Figure 1 — Resilience Management Policy in the Supply Chain (Source: Supply Chain Council 2007)

0.3 Process Approach

The management systems approach encourages organizations to analyse organizational and stakeholder requirements and define processes that contribute to success. A management system can provide the framework for continual improvement to increase the likelihood 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 fulfils organizational and stakeholder requirements.

This International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's resiliency to supply chain disruptions. 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 International Standard which 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 objectives,

d) monitoring and reviewing the performance and effectiveness of the resilience management policy, and

e) continual improvement based on objective measurement.

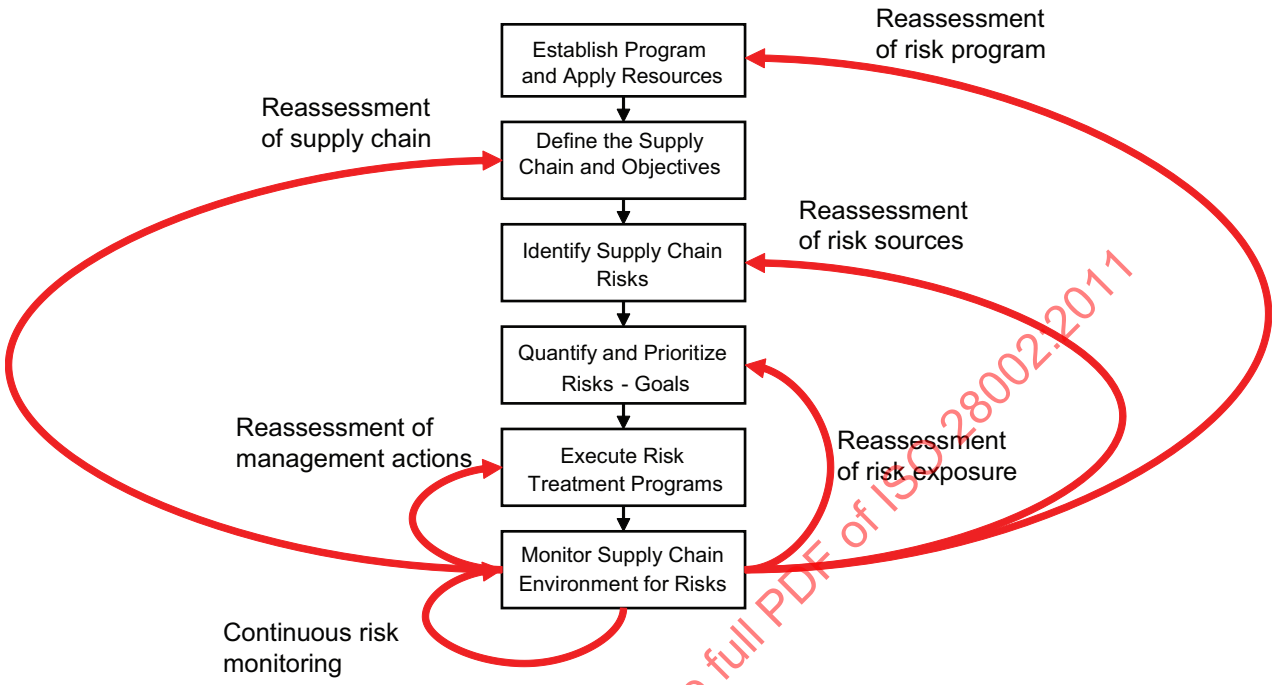

Figure 2 — Process Approach for Resilience Management in the Supply Chain

0.3.1 Establish a Supply Chain Resilience Program and Apply Resources

— Recognize supply chain risk management as a priority

— Secure top management support for the program and

— Secure resources necessary to execute the program

0.3.2 Define the Supply Chain and Resilience Objectives

— Define the supply chain scope and map the supply chain

— Define the objectives of managing risk in the subject supply chain

0.3.3 Identify Supply Chain Risks

— Comprehensively review the supply chain to identify risks

— Document identified risks to the extent possible

0.3.4 Quantify and Prioritize Risks

— Quantify each risk in terms of likelihood of occurrence and potential impact

— Use the quantification of the risks to prioritize the risks according to defined objectives

0.3.5 Execute Risk Treatment Programs

— Develop risk management actions consistent with each risk's priority

— Define each action's value in terms of reducing the likelihood and impact of the risk

— Develop and execute an implementation plan for the identified actions

0.3.6 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

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

This International Standard is designed to be incorporated into a management system that uses the "Plan-Do-Check-Act" (PDCA) model, which in turn will guide the implementation and execution of the resilience management policy processes. Figure 3 illustrates how a management system can incorporate a resilience management policy that captures the requirements and expectations of the interested parties and through the necessary actions and processes, produce risk management outcomes that meet those requirements and expectations. Figure 3 also illustrates the links in the processes presented in Clause 4 of this International Standard.

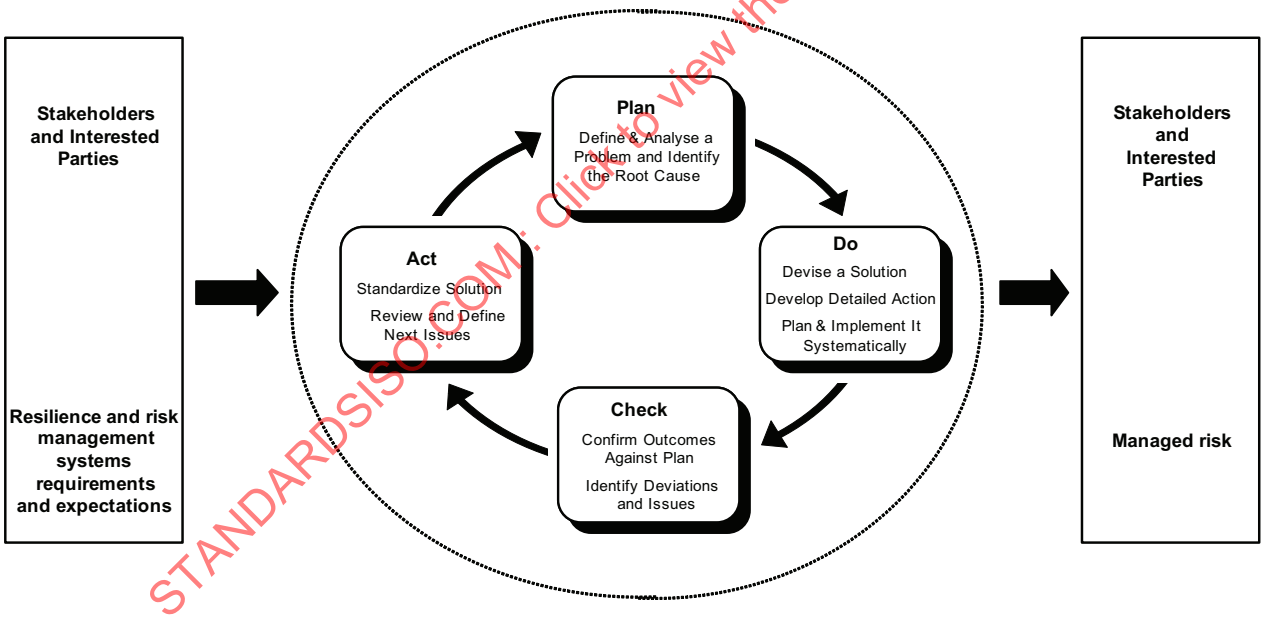

Figure 3 — Plan-Do-Check-Act Model

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 of a Management System that has incorporated this International Standard as a policy can be verified by an auditing process that is compatible and consistent with the methodology of ISO 28000:2007, ISO 14001:2004, and/or ISO/IEC 27001:2005, and the PDCA Model.

Additional information on qualifiers to application of this International Standard can be found in Annex D.

Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use

1 Scope

This International Standard specifies requirements for a resilience management policy in the supply chain to enable an organization to develop and implement policies, objectives, and programs, taking into account

— legal, regulatory and other requirements to which the organization subscribes,

— information about significant risks, hazards and threats that may have consequences to the organization, its stakeholders, and on its supply chain,

— protection of its assets and processes, and

— management of disruptive incidents.

This International Standard applies to risks 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 International Standard is applicable to any organization that wishes to

a) establish, implement, maintain, and improve a resilience management policy for the organization and its supply chain,

b) assure itself of its conformity with its stated resilience management policy,

c) demonstrate its management system contains a well developed Resilience Management Policy by:

   1) making a self-determination and self-declaration, or

   2) seeking confirmation of its conformance by parties having an interest in the organization (such as customers), or

   3) seeking confirmation of its self-declaration by a party external to the organization, or

   4) seeking certification/registration of that management system by an external organization.

All the requirements in this International Standard are intended to be incorporated into any type of the organization's management system that is based on the PCDA model. This International Standard provides the elements (including those addressing technology, facilities, processes, and people) required for this incorporation. The extent of the application of this International Standard will depend on factors such as the risk tolerance and policy of the organization; the nature and scale of its activities, products, and services; and the location where, and the conditions in which, the organization functions.

This International Standard provides generic requirements as a framework, applicable to all types of organizations (or parts thereof) regardless of size and function in the supply chain. This International Standard provides guidance for organizations to develop their own specific performance criteria, enabling the

organization to tailor and implement a resilience management policy appropriate to its needs and those of its stakeholders.

This International Standard emphasizes resilience, the adaptive capacity of an organization in a complex and changing environment, as well as protection of critical supply chain assets and processes. Applying this International Standard 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. This International Standard covers all phases of incident management before, during, and after a disruptive event.

This International Standard provides a framework for 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 International 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 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.

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

3 Terms and definitions

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

3.1
alternate worksite
work location, other than the primary location, to be used when the primary location is not accessible

3.2
asset
anything that has value to the organization

NOTE Assets include but are not limited to human, physical, information, intangible, and environmental resources.

3.3
audit
systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled

NOTE 1 Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the organization itself for management review and other internal purposes, and may form the basis for an organization's declaration of conformity. In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.

NOTE 2 External audits include those generally termed second- and third-party audits. Second-party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf. Third-party audits are conducted by external, independent auditing organizations, such as those providing certification/registration of conformity to ISO 28000, which is the supply chain security management system standard.

NOTE 3 When two or more management systems are audited together, this is termed a combined audit.

NOTE 4 When two or more auditing organizations cooperate to audit a single auditee, this is termed a joint audit.

3.4
auditor
person with the personal attributes and competence to conduct an audit

3.5
continual improvement
recurring activity to increase the ability to fulfil requirements

NOTE The process of establishing objectives and finding opportunities for improvement is a continual process through the use of audit findings and audit conclusions, analysis of data, management reviews or other means, and generally leads to corrective action or preventive action.

3.6
conformity
fulfilment of a requirement

3.7
consequence
outcome of an event affecting objectives

[ISO Guide 73:2009, definition 3.6.1.3]

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

3.8
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 International 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.

3.9
corrective action
action to eliminate the cause of a detected nonconformity

NOTE 1 There can be more than one cause for a nonconformity.

NOTE 2 Corrective action is taken to prevent recurrence whereas preventive action is taken to prevent occurrence.

3.10
crisis
unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment

3.11
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 the organization's 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 stay current and up-to-date.

3.12
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 can include individuals from the organization as well as immediate and first responders, stakeholders, and other interested parties.

3.13
critically
of essential importance with respect to objectives and/or outcomes

3.14
criticality analysis
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 in the continuity of the organization

3.15
disaster
event that causes great damage or loss

3.16
disruption
anticipated or unanticipated event that interrupts normal functions, operations, or processes (e.g. severe weather, political or labour unrest, utility outage, criminal/terrorist 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.

3.17
document
information and supporting medium

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

3.18
emergency
sudden, urgent, usually unexpected occurrence or event requiring immediate action

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

3.19
exercises
periodic events designed to evaluate the performance of team members and staff in the execution of resilience management policy

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 prevention, response and/or continuity procedures, but is more likely to involve the simulation of an incident, announced or unannounced, in which participants role-play in order to assess what issues might arise, prior to the actual occurrence of an incident.

3.20
evacuation
organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas to places of safety

3.21
event
occurrence or change of a particular set of circumstances

[ISO Guide 73:2009, definition 3.5.1.3]

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an “incident” or “accident”.

NOTE 4 An event without consequences can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

3.22
facility
plant, machinery, property, buildings, transportation units, sea/land/air ports, and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service

3.23
hazard
source of potential harm

[ISO Guide 73:2009, definition 3.5.1.4]

NOTE A hazard can be a risk source.

3.24
impact
evaluated consequence of a particular outcome

3.25
impact (consequence) analysis
process of analysing all operational functions and the effect that an operational interruption might have upon them

NOTE Impact analysis is part of the risk assessment process and 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 can be caused to the organization resulting from a disruption (or a change in the business or operating environment). Impact analysis identifies how the loss or damage will manifest itself; the degree for potential escalation of damage or loss with time following an incident; the minimum services and resources (human, physical, and financial) needed to enable business processes to continue to operate at a minimum acceptable level; and the timeframe and extent within which activities, functions, and services of the organization should be recovered.

3.26
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

3.27
integrity
property of safeguarding the accuracy and completeness of assets

3.28
likelihood
chance of something happening

[ISO Guide 73:2009, definition 3.6.1.1]

NOTE In risk management terminology, the word likelihood is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

3.29
management plan
clearly defined and documented plan of action, typically covering the key personnel, resources, services, and actions needed to implement the management process

3.30
mitigation
limitation of any negative consequence of a particular incident

3.31
mutual aid agreement
pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement

3.32
nonconformity
non-fulfilment of a requirement

3.33
objective
overall goal, consistent with the policy that an organization sets itself to achieve

3.34
organization
group of people and facilities with an arrangement of responsibilities, authorities, and relationships

EXAMPLE A public or private company, corporation, firm, enterprise, institution, charity, sole trader, association, or parts or combination thereof.

3.35
policy
overall intentions and direction of an organization as formally expressed by top management

NOTE This International Standard describes the requirements for one such policy (supply chain resilience policy).

3.36
preparedness
readiness
activities, programs, and systems developed and implemented prior to an incident that can be used to support and enhance prevention, protection from, mitigation of, response to, and recovery from disruptions, emergencies, or disasters

3.37
prevention
measures that enable an organization to avoid, preclude, or limit the likelihood or consequences of a disruption

3.38
preventive action
action to eliminate the cause of a potential nonconformity or other undesirable potential situation

NOTE 1 There can be more than one cause for a potential nonconformity.

NOTE 2 Preventive action is taken to prevent occurrence whereas corrective action is taken to prevent recurrence.

3.39
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 likelihood or consequences

3.40
probability
measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

[ISO Guide 73:2009, definition 3.6.1.4]

NOTE See also likelihood, 3.28.

3.41
procedure
specified way to carry out an activity or a process

NOTE 1 Procedures can be documented or not.

NOTE 2 When a procedure is documented, the term “written procedure” or “documented procedure” is frequently used. The document that contains a procedure can be called a “procedure document”.

3.42
record
document stating results achieved or providing evidence of activities performed

NOTE 1 Records can be used, for example, to document traceability and provide evidence of verification, preventive action and corrective action.

NOTE 2 Generally, records need not be under revision control.

3.43
residual risk
risk remaining after risk treatment

[ISO Guide 73:2009, definition 3.8.1.6]

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as “retained risk”.

3.44
resilience
adaptive capacity of an organization in a complex and changing environment

[ISO Guide 73:2009, definition 3.8.1.7]

NOTE 1 Resilience is the ability of an organization to prevent or 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.

3.45
resources
any asset (human, physical, information or intangible), facilities, equipment, materials, products or waste that has potential value and can be used

3.46
response plan
documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident

3.47
response program
plan, processes, and resources to perform the activities and services necessary to preserve and protect life, property, operations, and critical assets

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

3.48
response team
group of individuals responsible for developing, executing, rehearsing, and maintaining the response plan, including the processes and procedures

3.49
risk
effect of uncertainty on objectives

[ISO Guide 73:2009, definition 1.1]

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 be applied 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.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.

3.50
risk acceptance
informed decision to take a particular risk

[ISO Guide 73:2009, definition 3.7.1.6]

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

NOTE 2 Risks accepted are subject to monitoring and review.

3.51
risk analysis
process to comprehend the nature of risk and to determine the level of risk

[ISO Guide 73:2009, definition 3.6.1]

NOTE 1 Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2 Risk analysis includes risk estimation.

3.52
risk assessment
overall process of risk identification, risk analysis, and risk evaluation

[ISO Guide 73:2009, definition 3.4.1]

NOTE Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the likelihood 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.

3.53
risk communication
exchange or sharing of information about risk between the decision maker and other stakeholders

NOTE 1 Taken from ISO/IEC Guide 73:2002, definition 3.2.4, which has been withdrawn and replaced by ISO Guide 73:2009.

NOTE 2 The information can relate to the existence, nature, form, probability, severity, acceptability, treatment, or other aspects of risk.

3.54
risk criteria
terms of reference by which the significance of a risk is evaluated

[ISO Guide 73:2009, definition 3.3.1.3]

NOTE 1 Risk criteria are based on organizational objectives, and external and internal context.

NOTE 2 Risk criteria can be derived.

3.55
risk management
coordinated activities to direct and control an organization with regard to risk

[ISO Guide 73:2009, definition 2.1]

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

3.56
risk reduction
actions taken to lessen the probability, negative consequences, or both, associated with a risk

NOTE Taken from ISO/IEC Guide 73:2002, definition 3.4.4, which has been withdrawn and replaced by ISO Guide 73:2009.

3.57
risk sharing (transfer)
form of risk treatment involving the agreed distribution of risk with other parties

[ISO Guide 73:2009, definition 3.8.1.3]

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

NOTE 2 Risk sharing can be carried out through insurance or other forms of contract.

NOTE 3 The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

NOTE 4 Risk transfer is a form of risk sharing.

3.58
risk tolerance
organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives

[ISO Guide 73:2009, definition 3.7.1.3]

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

3.59
risk treatment
process to modify risk

[ISO Guide 73:2009, definition 3.8.1]

NOTE 1 Risk treatment can involve

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk,
- taking or increasing risk in order to pursue an opportunity,
- removing the risk source,
- changing the likelihood,
- changing the consequences, and
- sharing the risk with another party or parties (including contracts and risk financing), and retaining the risk by informed choice.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk limitation”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks.

3.60
security
condition of being protected against hazards, threats, risks, or loss

NOTE 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.

3.61
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

3.62
source
anything which alone or in combination has the intrinsic potential to give rise to risk

NOTE 1 Adapted from ISO/IEC Guide 73:2009, definition 3.5.1.2.

NOTE 2 A risk source can be tangible or intangible.

3.63
stakeholder (interested party)
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[ISO Guide 73:2009, definition 3.2.1.1]

NOTE 1 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.

NOTE 2 A decision maker can be a stakeholder.

3.64
supply chain
linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport

[ISO 28000:2007, definition 3.9]

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

3.65
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

NOTE Adapted from ISO 14001:2004, definition 3.12.

3.66
testing
activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria

NOTE 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.

3.67
threat
potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community

3.68
top management
person or group of people who directs and controls an organization at the highest level

3.69
vulnerability
intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence

[ISO Guide 73:2009, definition 3.6.1.6.]

3.70
vulnerability assessment
process of identifying and quantifying vulnerabilities

4 Requirements of Management System containing Resilience Policy

4.1 General

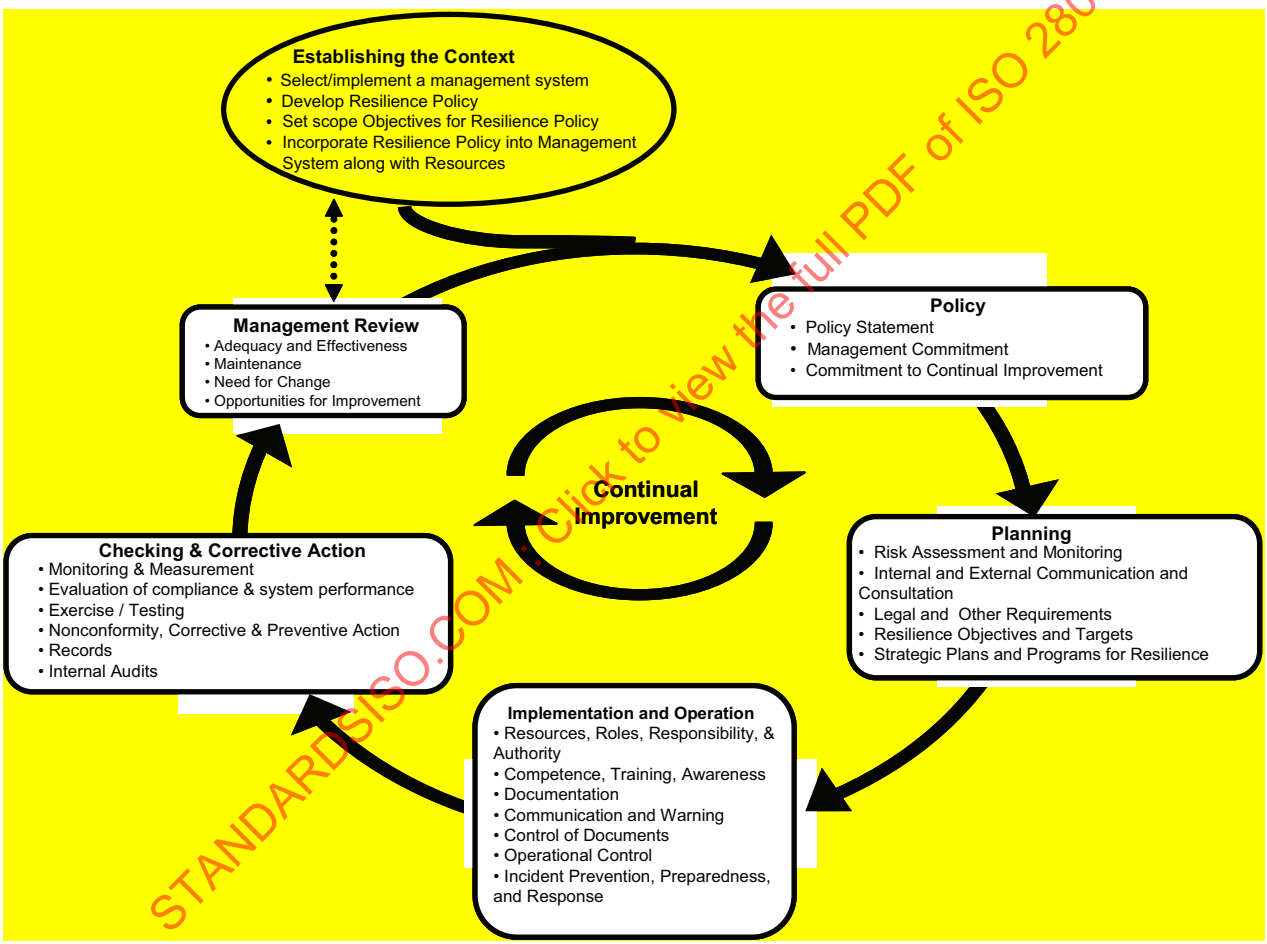

Figure 4 — Management System containing Resilience Policy Flow Diagram

The organization shall establish a supply chain resilience policy in accordance with the requirements of this International Standard. For this policy to be effective it should be incorporated within a management system. Where requirements identical to the requirements of this International Standard have been previously addressed during the adoption of the management system into which this International Standards' requirements will be incorporated, those requirements do not need to be repeated separately.

4.2 Understanding the Organization and its Context

4.2.1 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, social, 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 an 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).

4.2.2 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 within one or more of its supply chains;

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.

4.3 Scope of Resilience Management Policy

The organization shall define and document the objectives and scope of its resilience management policy 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 policy, as either 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 objectives, 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, based both on potential internal and external disruptions that could adversely affect the operations and functions of the organization within the context of their potential likelihood and impact,

e) define scope of the resilience management policy 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.).

The organization shall also assign strategic weights to 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 (see 4.4).

4.4 Provision of Resources for the Resilience Management Policy

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

4.5 Resilience Management Policy

Top management shall define, document, and provide resources for the organization's management system into which the resilience management policy has been incorporated, reflecting a commitment to the protection of human, environmental, and physical assets; anticipating and preparing for potential adverse events; and business and operational resilience.

4.6 Resilience Policy Statement

The organization adopting this International Standard shall produce a resiliency policy statement to be incorporated into its management system. The resiliency policy statement shall be 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.

The policy shall

a) include a commitment to employee and community life safety as the first priority,

b) include a commitment to continual improvement,

c) include a commitment to enhanced organizational and supply chain sustainability and resilience,

d) include a commitment to adaptive and proactive risk minimization,

e) include a commitment to comply with applicable legal requirements and with other requirements to which the organization subscribes,

f) determine and document the risk tolerance in relation to the scope of the management policy and address and specify where in the management system adopted by the organization the following related to resiliency management are addressed:

g) a framework for setting and reviewing resilience management policy objectives and targets;

— references to limitations and exclusions;

— a designated policy owner and/or responsible point of contact;

— how it is documented, implemented and maintained;

— how it is communicated to all appropriate persons working for or on behalf of the organization;

— how it is made available to relevant stakeholders;

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

— how it is reviewed at planned intervals and when significant changes occur; and

— how it is visibly endorsed by top management.

Annex A
(informative)

Informative guidance on the incorporation of this International Standard into a management standard

A.1 General

Organizations adopting this International Standard are required to incorporate the Resilience Management Policy into a management system that is based on the PDCA model. The Resilience Management Policy may be one of many policies adopted by the organization in their setting of overall management policy. The Resilience Management Policy becomes an input into the organization's management system. The documentation, implementation, resource needs and management of execution of each corporate management policy is required to be documented in recognized management systems. This annex provides informative guidance on incorporating the elements of the Resilience Management Policy into a PDCA type management system. If other policies are also being included in the management system, appropriate guidance should be sought to address them as well.

A.2 Resilience Management Policy

The Resilience Management Policy should be developed and documented in accordance with this International Standard. The Policy should be added to the policies that are part of the overall management system.

A.3 Management Commitment

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

a) Establishing a resilience management policy;

b) Ensuring that resilience management policy objectives and plans are established;

c) Establishing roles, responsibilities, and competencies for resilience management functions;

d) Appointing one or more persons to be responsible for the resilience management policy 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 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 policy;

g) Deciding the criteria for accepting risks and the acceptable levels of risk;

h) Ensuring that internal resilience management policy audits are conducted;

i) Conducting management reviews of the resilience management policy; and

j) Demonstrating its commitment to continual improvement.

A.4 Planning

A.4.1 Risk Assessment and Monitoring

The organization should 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 (including likelihood, vulnerability, criticality, and impacts/consequences);

c) To determine those risks that have a significant consequence on activities, functions, services, products, supply chain, stakeholder relationships, and the environment; and

d) To systematically evaluate and prioritize risk controls and treatments and their related costs.

The organization should:

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 organization's internal and external context;

c) Ensure that the prioritized risks are taken into account in establishing, implementing, and operating its resilience management system;

d) Re-evaluate risk within the context of changes within the organization or made to the organization's operating environment, procedures, functions, services, partnerships, and supply chains;

e) 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;

f) 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;

g) Establish a prioritized timeframe for recovery of activities and functions within the organization and throughout the supply chain; and

h) Evaluate the direct and indirect benefits and costs of options to reduce risk and enhance sustainability and resilience.

A.4.2 Internal and External Communication and Consultation

The organization should 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) risks 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.

A.4.3 Monitoring and Reviewing the Risk Assessment Process

The organization should 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 affect on the risk assessment of the context, assumptions and other factors that may change over time due to internal and external circumstances;

c) evaluate the effectiveness of risk controls and treatments; and

d) evaluate the actual effectiveness post-incident.

A.4.4 Legal and Other Requirements

The organization should establish and maintain procedure(s) to

a) 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) Determine how these requirements apply to its hazards, threats, risks and their potential impacts.

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

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

A.4.5 Resilience Objectives and Targets

The organization should 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 should 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 should be derived from and consistent with the resilience management policy and risk assessment, including the commitments to:

a) Minimize risk by reducing likelihood and consequence;

b) Increased resilience through adaptive, proactive and reactive approaches; financial, operational and business requirements (including supply chain commitments);

c) Compliance with legal and other requirements; and

d) Continual improvement.

When establishing and reviewing its objectives and targets, an organization should consider the legal, regulatory, and other requirements; its significant risks; 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 should be derived from and consistent with the resilience management policy objectives and should be:

a) to an appropriate level of detail;

b) commensurate to the risk assessment and the organization's timeframe for recovery;

c) specific, measurable, achievable, relevant and time-based (where practicable);

d) 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;

e) reviewed periodically to ensure that they remain relevant and consistent with the resilience management policy objectives and amended accordingly.

A.4.6 Strategic Plans and Programs for Resilience

The organization should establish, implement and maintain one or more strategic program(s) for achieving its objectives and targets. The programs should be optimized and prioritized in order to control and treat risks associated with the likelihood and impacts of disruptions to the organization and its supply chain. The program(s) should 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, time-frame and resource allocation by which the resilience management objectives and targets are to be achieved.

The organization should 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 should be reviewed periodically to ensure that they remain effective and consistent with the objectives and targets. Where necessary, the programs should be amended accordingly.

A.5 Implementation and Operation

A.5.1 Resources, Roles, Responsibility and Authority for Resilience Management

Roles, responsibilities and authorities should 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 should appoint specific management representative(s) who, irrespective of other responsibilities, should have defined roles, responsibilities, and authority for:

a) Ensuring that a resilience management policy is established, communicated, implemented, and maintained in accordance with the requirements of this International 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 policy to top management for review and as the basis for improvement.

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

a) Established to ensure that fiscal decisions can be expedited; and

b) In accordance with established authority levels and accounting principles.

A.5.2 Competence, Training, and Awareness

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

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

The organization should establish, implement, and maintain procedure(s) to ensure all 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 supply chain security management system;

d) Their roles and responsibilities in achieving conformity with the requirements of the resilience management policy;

e) The potential consequences of departure from specified procedures; and

f) The benefits of improved personal performance.

The organization should 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.

A.5.3 Communication and Warning

With regard to its hazards, threats, risks and resilience management policy, the organization should 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 should 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 document its decision. If the decision is to communicate, the organization should establish and implement method(s) for this external communication, alerts, and warnings (including with the media).

The resilience management policy communications systems should be regularly tested.

A.5.4 Documentation

The resilience management policy documentation should include:

a) The resilience management policy, objectives, and targets;

b) Description of the scope of the resilience management policy;

c) Description of the main elements of the resilience management policy and their integration with related documents;

d) Documents, including records, required by this International 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 should determine the security sensitivity of information and should take appropriate steps to prevent unauthorized access.

A.5.5 Control of Documents

Documents required by the resilience management policy should be controlled. *Records* are a special type of document and should be controlled in accordance with the requirements given in A.5.4.

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

a) Comply with legal and regulatory requirements;

b) Approve documents for adequacy prior to issue;

c) Review, update and re-approve documents as necessary;

d) Ensure that changes and the current revision status of documents are identified;

e) Ensure that relevant versions of applicable documents are available at points of use;

f) Establish document retention, archival, and destruction parameters;

g) Ensure that documents remain legible and readily identifiable;

h) Ensure that documents of external origin determined by the organization to be necessary for the planning and operation of the resilience management policy are identified and their distribution controlled;

i) Identify as obsolete all out-of-date documents that the organization is required to retain; and

j) 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.5.6 Operational Control

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

a) The resilience management policy;

b) The control of activities identified as having significant risk;

c) Compliance with legal and regulatory requirements;

d) Its resilience management policy objectives;

e) The delivery of its resilience management policy programs; and,

f) The required level of supply chain resilience.

The organization should 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, 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 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 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 should 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 should consider the associated risks before their implementation. The new or revised arrangements to be considered should 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 should:

a) Address reliability and resilience, 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);

e) Be commensurate with the supply chain resilience objectives and fit for purpose; and

f) 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.

A.5.7 Incident Prevention, Preparedness and Response

A.5.7.1 General

The organization should establish, implement, and maintain 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) should document how the organization will prevent, protect from, prepare for, mitigate, respond to and recover from disruptive incidents. The organization should 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 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 should periodically review and, where necessary, revise its incident prevention, preparedness, response, and recovery procedures – in particular, after exercises or the occurrence of accidents or incidents that can escalate into an emergency, crisis, or disaster.

The organization should 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 should document this information and update it at regular intervals or as changes occur.

A.5.7.2 Incident Prevention, Preparedness, and Response Structure

The organization should 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 should 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.

A.5.7.3 Incident Prevention, Protection and Mitigation

The organization should 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 should 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 risk exposure;

b) reduce the risk by modifying activities, processes, equipment or materials;

c) isolate or separate the assets from risk;

d) engineering controls to detect, deter, and delay a potential hazard or threat agent;

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

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

A.5.7.4 Incident Response

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

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

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

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

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

e) effective in minimizing consequences through implementation of appropriate mitigation plans; and

f) consider the transition of post-incident management that contributes to the resumption and recovery of operations.

A.5.7.5 Incident 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.

Each plan should 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 should 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.

A.6 Checking and Corrective Action

A.6.1 General

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

A.6.2 Monitoring and Measurement

The organization should establish, implement, and maintain performance metrics and 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) should include the documenting of information to monitor performance, applicable operational controls, and conformity with the organization's resilience management objectives and targets.

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

A.6.3 Evaluation of Compliance and System Performance

A.6.3.1 Evaluation of Compliance

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

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

A.6.3.2 Exercises and Testing

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

The organization should validate its resilience management policy 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 the risk assessment and 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.

A.6.4 Nonconformity, Corrective Action, and Preventive Action

The organization should establish, implement, and maintain procedure(s) for dealing with actual and potential nonconformity(ies) and for taking corrective action and preventive action. The procedure(s) should 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) Implement corrective action(s) and preventive action(s)

e) Recording the results of corrective action(s) and preventive action(s) taken; and

f) Reviewing the effectiveness of corrective action(s) and preventive action(s) taken.

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

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

The priority of preventive actions should be determined based on the results of the risk assessment.

The organization should make any necessary changes to the resilience management policy documentation.

A.6.5 Control of Records

The organization should establish and maintain records to demonstrate conformity to the requirements of its resilience management policy and the results achieved.

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

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

A.6.6 Internal Audits

The organization should conduct internal resilience management system policy 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 policy:

a) Conform to the requirements of this International 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 should 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 should be defined. The selection of auditors and conduct of audits should ensure objectivity and impartiality of the audit process. Auditors should not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see A.6.5), should be defined in a documented procedure.

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

A.7 Management Review

A.7.1 General

Management should review the organization's overall security management system at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. This review should include assessing opportunities for improvement and the need for changes to the management system, including the resilience management system policy and objectives. The results of the reviews should be clearly documented and records should be maintained (see A.6.5).

A.7.2 Review Input

The input to a management review should include:

a) Results of resilience management system policy 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 policy;

j) Adequacy of policy and objectives; and

k) Recommendations for improvement.

A.7.3 Review Output

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

a) Improvement of the effectiveness of the management policy;

b) Update of the risk assessment, 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 affect the resilience management policy, including changes to:

   1) Business and operational requirements;

   2) Risk reduction and security requirements;

   3) Operational conditions processes effecting the existing operational requirements;

   4) Regulatory or legal requirements;

   5) Contractual obligations; and

   6) Levels of risk and/or criteria for accepting risks;

d) Resource needs; and

e) Improvement of how the effectiveness of controls is being measured.

A.7.4 Maintenance

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

A.7.5 Continual Improvement

The organization should continually improve the effectiveness of the 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 B
(informative)

Informative Guidance on the Use of this International Standard

B.1 Introduction

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

Natural disasters, environmental accidents, technology mishaps, and manmade 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 ongoing, 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 International Standard provides organizations of all sizes with the resilience policy 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.

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 International Standard provides guidance or recommendations for any organization 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 their risks and their 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 operational 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 its management system depends on the commitment of all levels of management 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 of disruptive events. 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, its leadership has a duty to stakeholders to plan for its survival.

B.2 General Guidance

A management system is a dynamic and multifaceted process, with each element interacting as a structured set of functional units. It provides a framework that is based on the premise that the component parts of a system can best be understood when viewed in the context of relationships with each other and with other systems, rather than in isolation. The only way to fully understand and implement the elements of a management system is to understand that part in relation to the whole. Therefore, it should be noted that a management system is not a simple cycle, but rather a complex set of interrelated elements interacting with each other. This results in an iterative process where establishing the context and policy, risk assessment, implementation and operation, evaluation and review are not a series of consecutive steps but rather a network of interacting functions.

The management systems approach is characterized by:

— Understanding the context and environment within which the system operates;

— Identifying the core elements of the system, as well as the system boundary;

— Understanding the role or function of each element in the system; and,

— Understanding the dynamic interaction between elements of the system.

The systems approach ensures that holistic strategies and policies are developed. It provides a sound analytical basis for developing strategies and policies that are to be implemented in the complex and changing environment in which the organization operates. Establishing a framework for assessing the risks and effectiveness of strategies and policies prior to and during implementation provides a feedback loop for decision-making throughout the process.

The implementation of an organizational resilience (OR) management policy specified by this International Standard is, together with a management system, intended to result in improved security, preparedness, response, continuity, and recovery performance. Therefore, this International Standard is based on the premise that the organization will periodically review and evaluate its management system and resilience policy 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 management system are intended to result in further improvements in security, preparedness, response, continuity, and recovery performance, and the organization's resilience. This International 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 risks 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 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.

B.3 Understanding the Organization and its context

In order for the organization to design and implement a management system with a resiliency policy to manage its risks and that of its supply chain, the organization must first evaluate and understand the internal and external context in which it operates. When establishing the resiliency policy within a management context, the organization should consider the internal and external parameters relevant to the organization and its supply chain (see Figure B.1). 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.

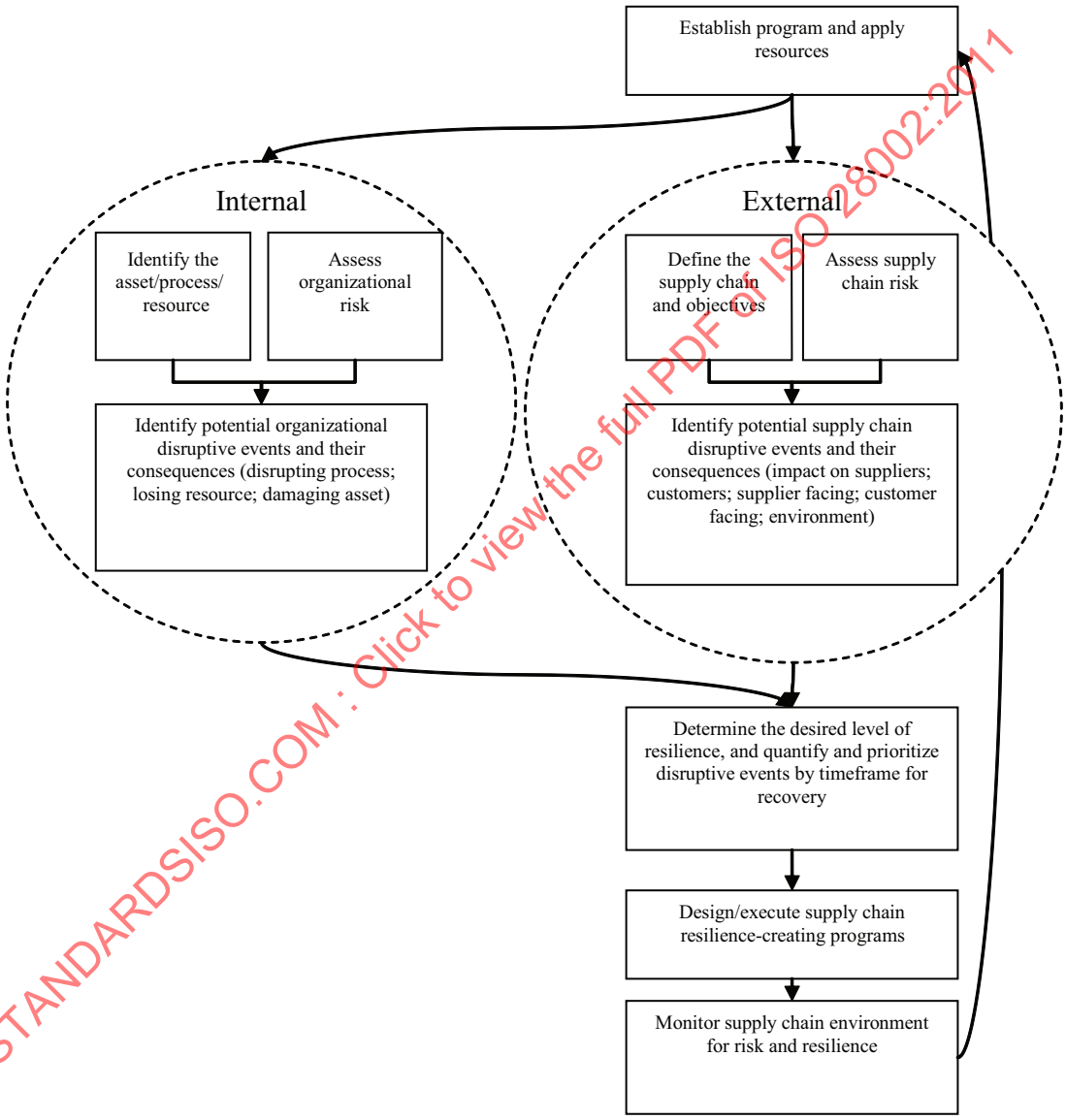

Figure B.1 — Understanding the Context for Resilience Management in the Supply Chain

B.4 Scope of Resilience Management Policy

An organization has the freedom and flexibility to define its boundaries, and may choose to implement this International 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 policy.

Scoping is intended to clarify the boundaries of the organization and nodes of the supply chain to which the resilience management policy 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 policy. In setting the scope, the credibility of the resilience management policy will depend upon the choice of organizational boundaries. Where a part of an organization is excluded from the scope of its resilience management policy, the organization should be able to explain the exclusion.

If this International 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 International 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 International 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 (see A.4.1).

B.5 Provision of Resources for the Resilience Management Policy

The resources needed for the resilience management policy 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.

B.6 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) The 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 ensure 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.

B.7 Planning

B.7.1 Risk Assessment and Monitoring

The risk assessment process provides decision makers with an improved understanding of the risks that could affect achievement of its operational and business objectives, and that of its supply chain. It is intended to create a systematic process for an organization to identify critical assets, hazards, threats, vulnerabilities, 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 policy. The risk assessment provides the foundation for setting objectives, targets and programs within the security management system, as well as measuring the efficacy of the resilience management.

An organization should apply ISO 31000:2009 (Figure B.2).

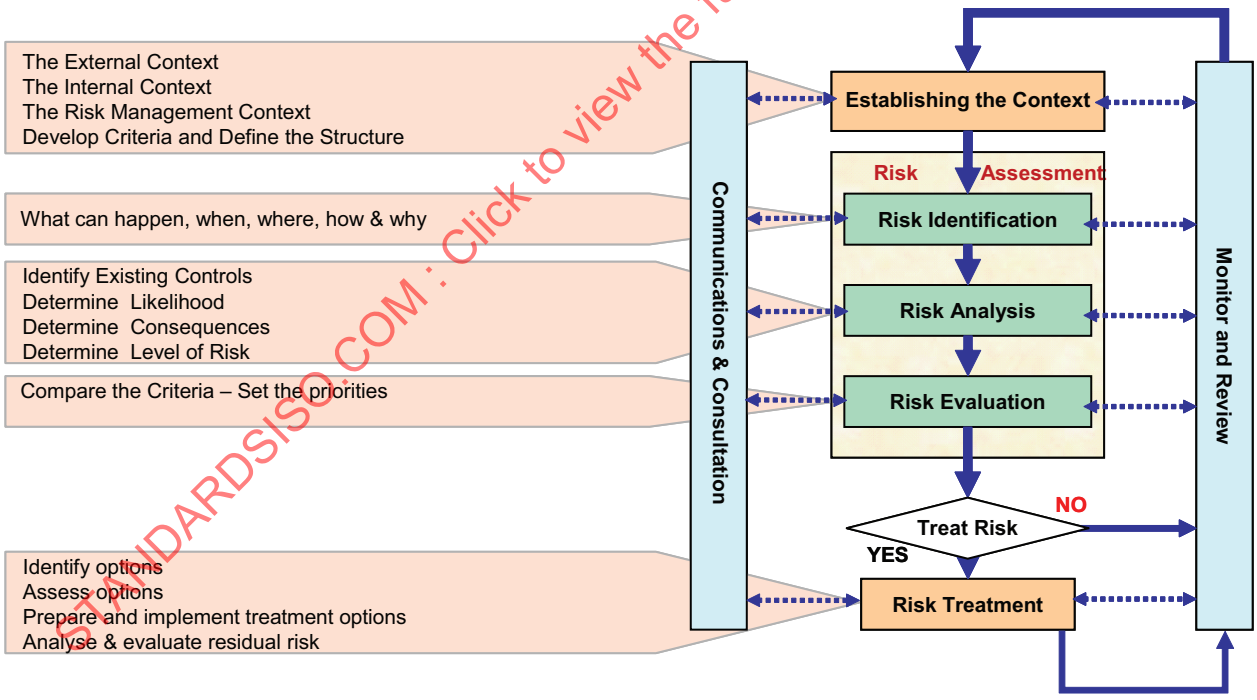

Figure B.2 — Process for Managing Risk

Establishing the context allows the organization to determine what it is that they believe they need to protect and defines a grading system for the risk assessment elements to ensure consistency.

External Context includes

— Cultural, political, legal, regulatory, financial, natural, business arena (International, National, Local)

— Key drivers and trends having an impact on objectives

— Perceptions and values of external stakeholders

Internal Context includes

— Capabilities understood in terms of resources and knowledge (people, processes, systems, technology, time and capital)

— Information – systems, flows and decision-making processes

— Internal stakeholders

— Objectives and strategies of the organization

— Perception, values and culture

— Policies and processes

— Standards, reference models, structures (governance, roles and accountabilities)

— Agreed processes for risk assessment objectives, risk criteria [vulnerabilities, hazards (threats) likelihood and consequence], risk assessment program and timing.

During the process of establishing the internal and external context, the organization should identify comprehensively all the significant assets of the organization. This includes identifying the relative importance of various types of asset to the viability and success of the organization. This should include people, property, information, processes, activities and intangibles (e.g. market share or position, reputation, credibility, etc.). Property may include built structures and/or equipment crucial to the operations of the organization. Organizations may select categories of activities, products, and services to identify their criticality, risks, and impacts.

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.

   The identification of plausible threats/hazards involves the proactive gathering of intelligence in relation to potential sources of harm. Threats/hazards may include but are not limited to harmful persons, financial factors, competitor or supplier influences, business activity or other situations internal or external to the organization.

   The vulnerability evaluation identifies those weaknesses that exist in the physical, procedural and operational activities that may allow or improve the opportunity for the threat to be realized.

b) Risk analysis: is the process of developing and understanding 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 the incident and associated consequences can occur.

   An organization should determine what the consequences or impact of an incident upon a site or facility would be were a threat to be realized. The consequences may be categorized based on death or injury to human life, financial or operational impact, business interruption, structural damage and damage to intangibles (reputation, brand name, credibility, industry and public positioning).

   This process of consequence determination may also be known as impact analysis.

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.

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 (including their criticality) related to 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 the dependencies of others 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) Analyse 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) Analyse 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, 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. 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 analyse 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 non-functional 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, 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 policy.

The process of identification and evaluation of risks 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 is not intended to change or increase an organization's legal obligations.

B.7.2 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 labelling 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.

B.7.3 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.

B.7.4 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 policy. 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.

B.8 Implementation and Operation (Tactical Implementation)

B.8.1 Resources, Roles, Responsibility, and Authority

The successful implementation of a resilience management policy 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 policy 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 policy. 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, 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 be 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.

B.8.2 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 International Standard states the following:

a) The importance of conformity with the resilience management policy and procedures and with the requirements of the overall 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 policy;

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 be 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 at 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 – be familiar with relevant parts of the response plans.

B.8.3 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 funnelled 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.

B.8.4 Documentation

The level of detail of the documentation should be sufficient to describe the resilience management policy 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 policy. 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.