PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 28002

First edition
2010-09-01

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/PAS 28002:2010(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;
- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

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

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

ISO/PAS 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.

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 ensure 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 Publicly Available Specification 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 Publicly Available Specification provides generic auditable criteria to establish, check, maintain, and improve management policy when implemented in a management system to enhance prevention, preparedness (readiness), mitigation, response, continuity, and recovery from disruptive incidents.

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

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 program. With this understanding, an organization will define to which level or tier in their supply chain to include in their resilience program.

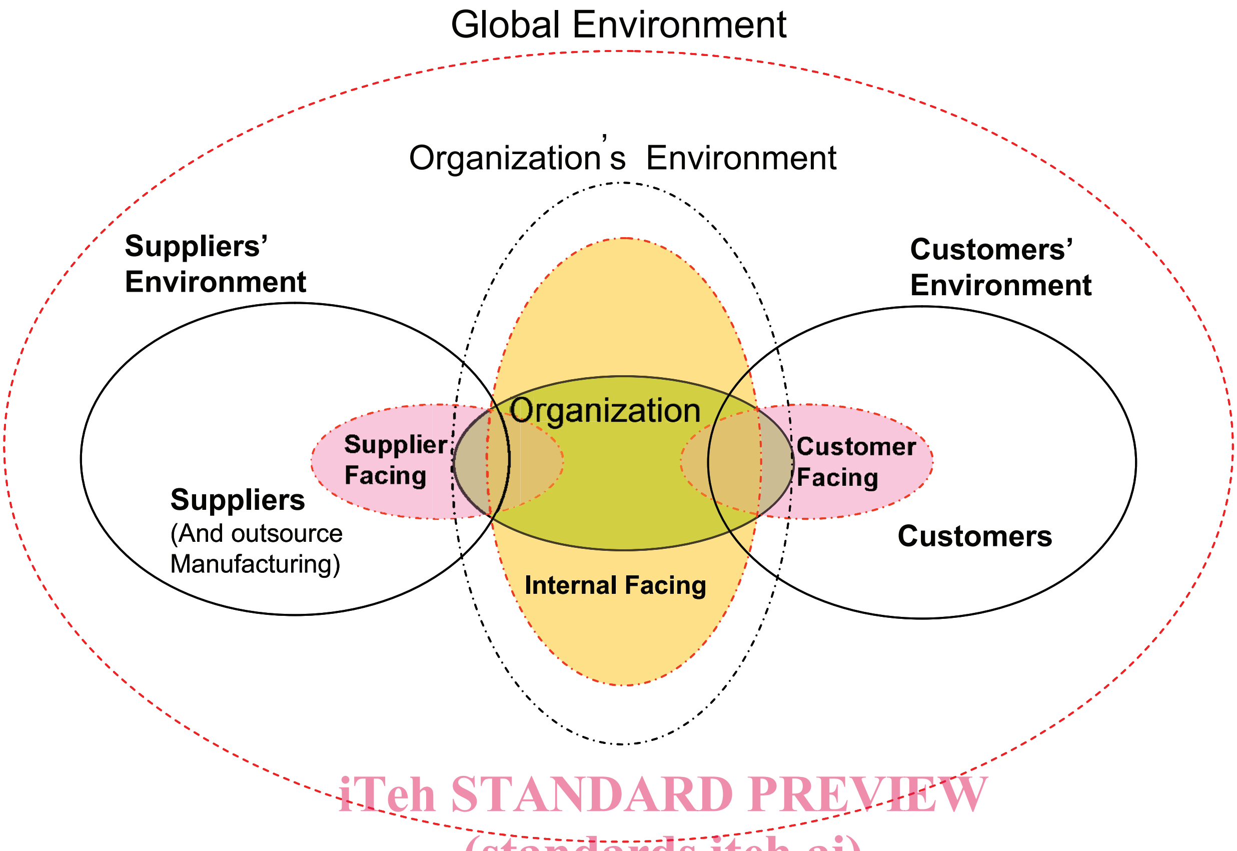

Figure 1 — Resilience management in the supply chain

0.3 Process approach

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

This Publicly Available Specification 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 Publicly Available Specification, 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 system, and

e) continual improvement based on objective measurement.

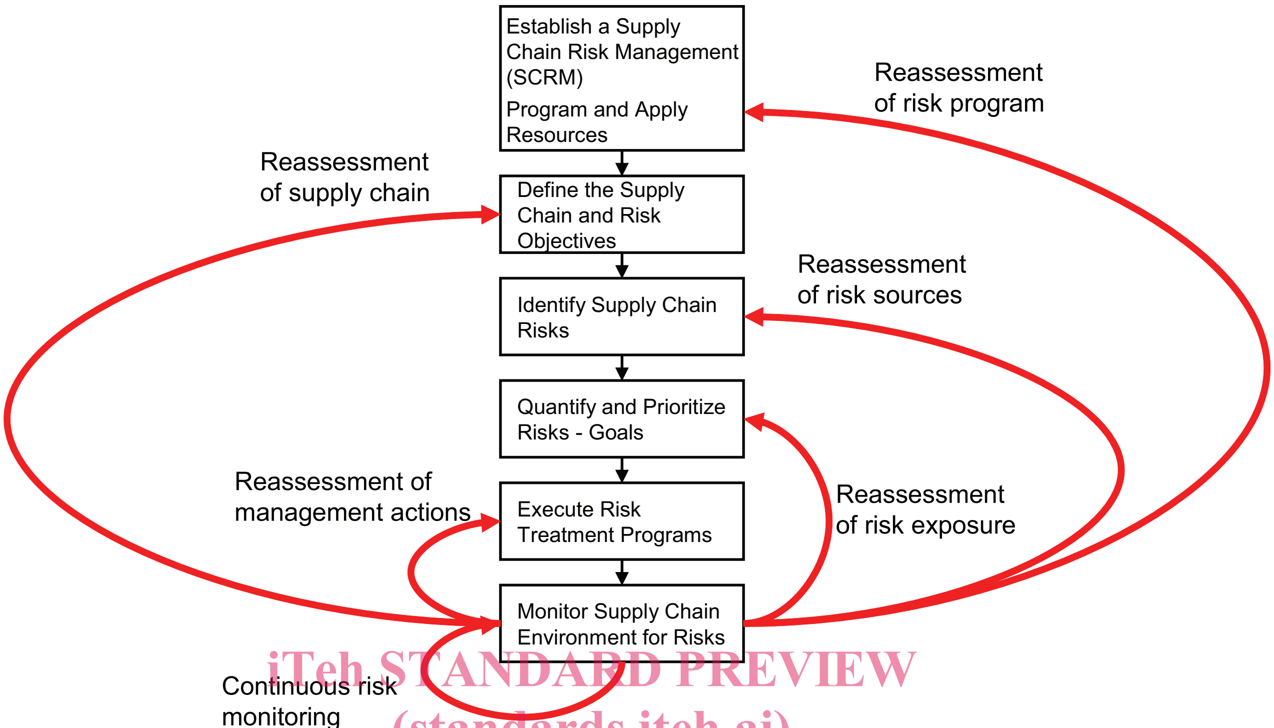
Establish a Supply Chain Risk Management (SCRM)
Program and Apply Resources
Define the Supply Chain and Risk Objectives
Identify Supply Chain Risks
Quantify and Prioritize Risks - Goals
Execute Risk Treatment Programs
Monitor Supply Chain Environment for Risks
Reassessment of risk program
Reassessment of supply chain
Reassessment of risk sources
Reassessment of management actions
Reassessment of risk exposure
Continuous risk monitoring

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 Publicly Available Specification 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 resilience management policy that captures the requirements and expectations of the interested parties and, through the necessary actions and processes, can 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 Publicly Available Specification.

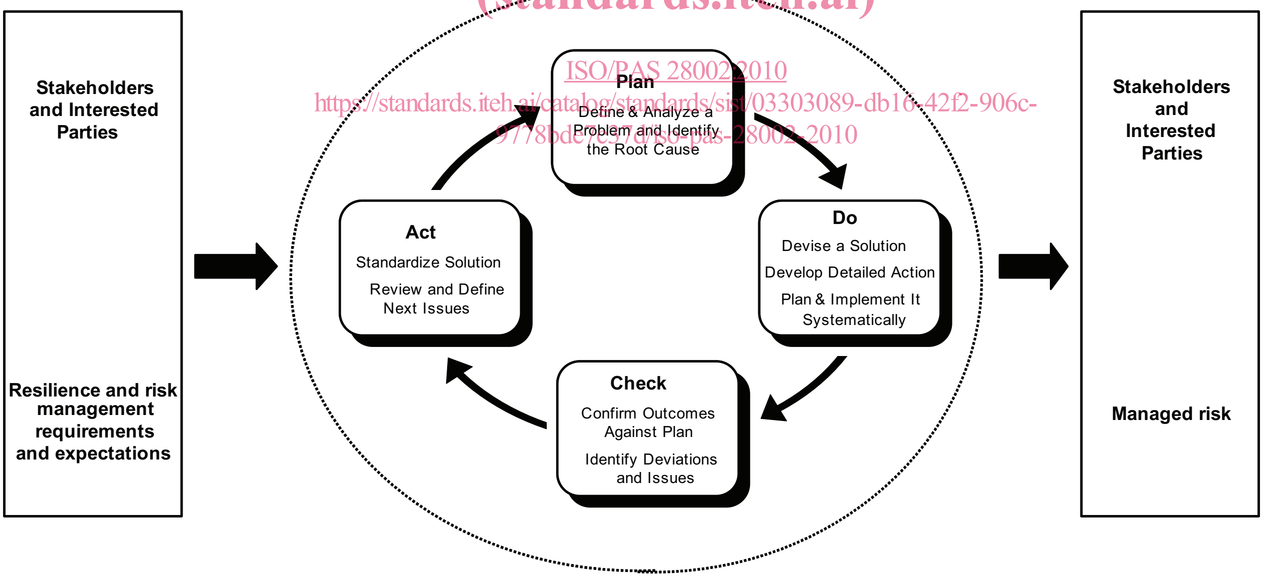
Stakeholders and Interested Parties
Resilience and risk management requirements and expectations
Plan
Define & Analyze a Problem and Identify the Root Cause
Do
Devise a Solution
Develop Detailed Action Plan & Implement It Systematically
Check
Confirm Outcomes Against Plan
Identify Deviations and Issues
Act
Standardize Solution
Review and Define Next Issues
Stakeholders and Interested Parties
Managed risk

Figure 3 — PDCA 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 Publicly Available Specification as a policy can be verified by an auditing process that is compatible and consistent with the methodology of ISO 9001:2000, ISO 14001:2004, ISO 28000:2007 and/or ISO/IEC 27001:2005, and the PDCA Model.

Additional information on qualifiers to application of this Publicly Available Specification 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 Publicly Available Specification specifies requirements for a resilience management system in the supply chain to enable an organization to develop and implement policies, objectives, and programs, taking into account

a) legal, regulatory and other requirements to which the organization subscribes,

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

c) protection of its assets and processes, and

d) management of disruptive incidents.

This Publicly Available Specification 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 Publicly Available Specification is applicable to any organization that wishes to

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

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

c) demonstrate their management system contains a well-developed resilience management policy by

- making a self-determination and self-declaration, or
- seeking confirmation of its conformance by parties having an interest in the organization (such as customers), or
- seeking confirmation of its self-declaration by a party external to the organization, or
- seeking certification/registration of its resilience management system by an external organization.

All the requirements in this Publicly Available Specification are intended to be incorporated into any type of the organization's management system that is based on the PDCA (plan-do-check-act) model. This Publicly Available Specification provides the elements (including those addressing technology, facilities, processes, and people) required for this incorporation. The extent of the application of this Publicly Available Specification 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 Publicly Available Specification 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 Publicly Available Specification provides guidance for organizations to develop their own specific performance criteria, enabling the organization to tailor and implement a resilience management system appropriate to its needs and those of its stakeholders.

This Publicly Available Specification 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 Publicly Available Specification 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 Publicly Available Specification covers all phases of incident management before, during, and after a disruptive event.

This Publicly Available Specification provides a framework for an organization to

i) develop a prevention, protection, preparedness, mitigation and response/continuity/recovery policy,

ii) establish objectives, procedures, and processes to achieve the policy commitments,

iii) assure competency, awareness, and training,

iv) set metrics to measure performance and demonstrate success,

v) take action as needed to improve performance,

vi) demonstrate conformity of the system to the requirements of this Publicly Available Specification, and

vii) 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.

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 fulfill 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
fulfillment 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 Publicly Available Specification, 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 may 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 on 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 labor 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