BS ISO 28002:2011

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO 28002:2011.

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

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

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

© BSI 2011

ISBN 978 0 580 70768 1

ICS 03.100.10; 47.020.99

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2011.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 28002:2011

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)

Documents
Document Sharing Hub

© ISO 2011

Full document details: BS ISO 28002:2011

COPYRIGHT PROTECTED DOCUMENT

© ISO 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2011 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 28002:2011

Contents

Page

Foreword iv

Introduction v
0.1 General v
0.2 Supply Chain Environment v
0.3 Process Approach vi
0.4 "Plan-Do-Check-Act" (PDCA) model viii

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Requirements of Management System containing Resilience Policy 12
4.1 General 12
4.2 Understanding the Organization and its Context 13
4.3 Scope of Resilience Management Policy 14
4.4 Provision of Resources for the Resilience Management Policy 14
4.5 Resilience Management Policy 14
4.6 Resilience Policy Statement 14

Annex A (informative) **Informative guidance on the incorporation of this International Standard into a management standard** 16

Annex B (informative) **Informative Guidance on the Use of this International Standard** 30

Annex C (informative) **Terminology Conventions** 53

Annex D (informative) **Qualifiers to Application** 54

Bibliography 55

© ISO 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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.

© ISO 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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.

Documents
Document Sharing Hub

© ISO 2011 – All rights reserved

Full document details: BS ISO 28002:2011

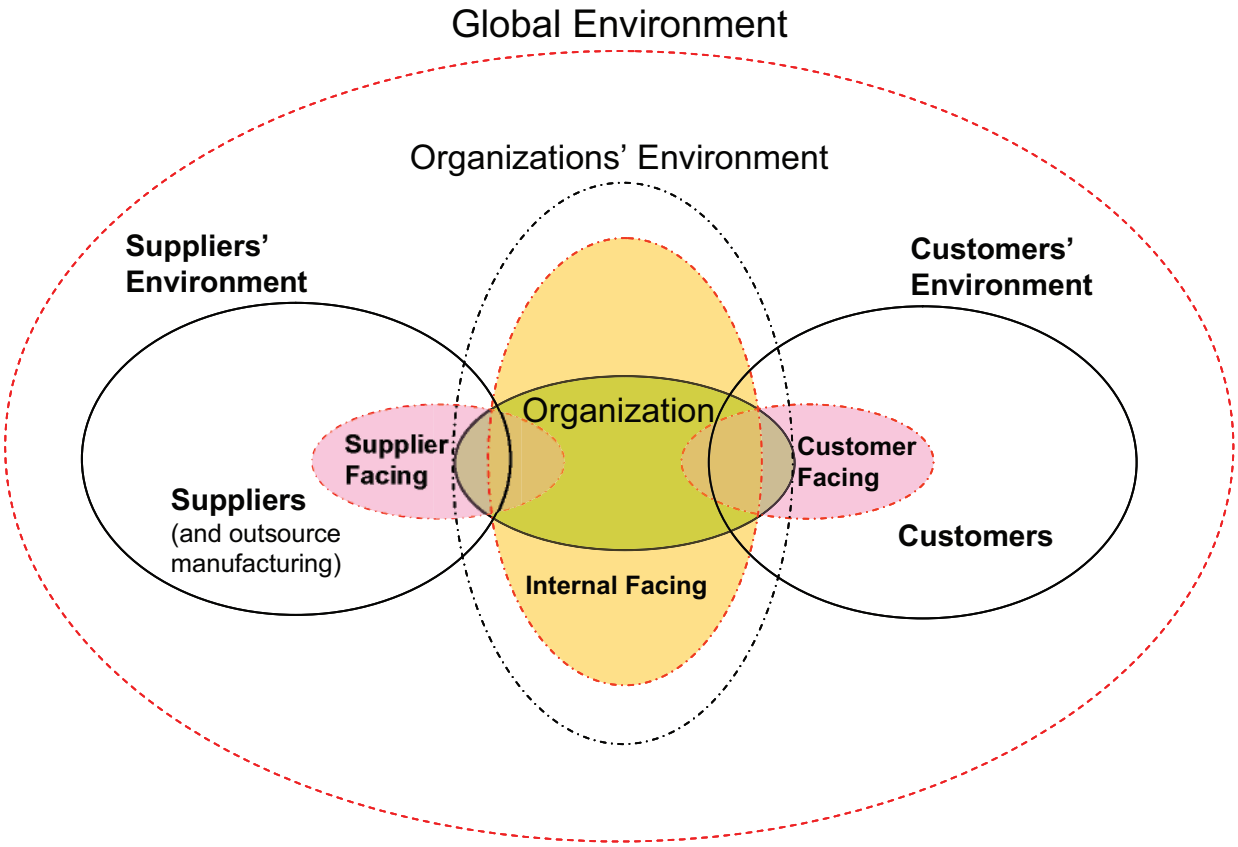

Figure 1 — Resilience Management Policy in the Supply Chain (Source: Supply Chain Council 2007)

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,

© ISO 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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

e) continual improvement based on objective measurement.

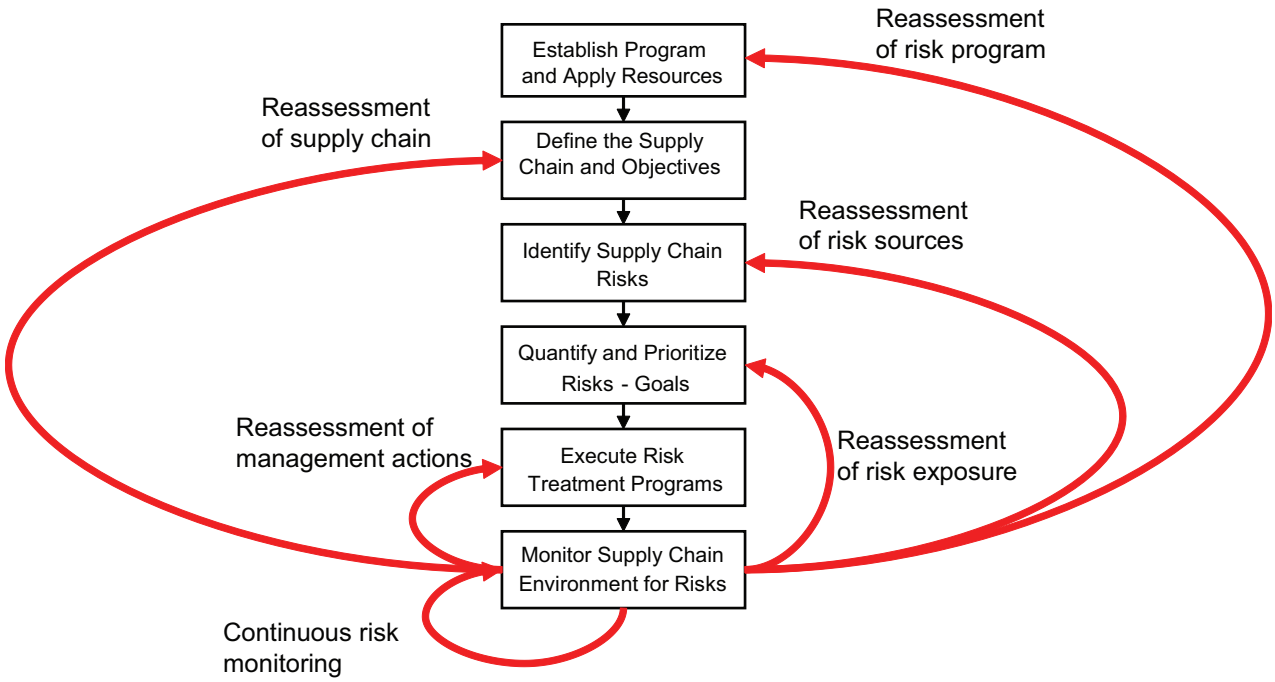

Figure 2 — Process Approach for Resilience Management in the Supply Chain

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

© ISO 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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.

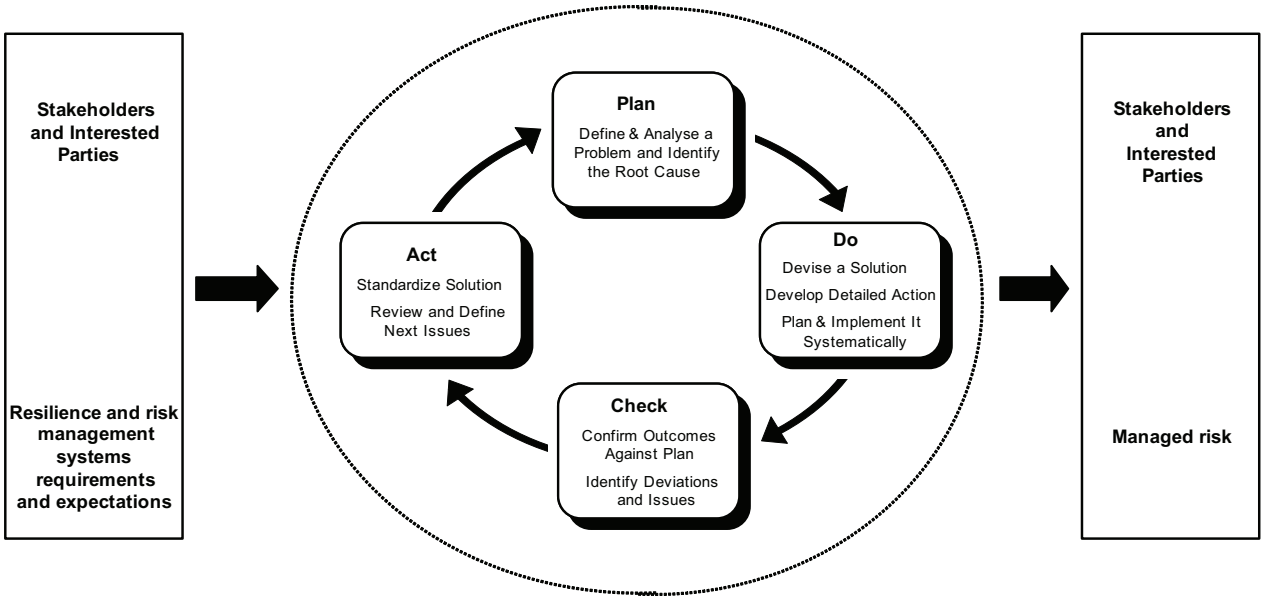

Figure 3 — Plan-Do-Check-Act Model

© ISO 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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.

© ISO 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

Documents
Document Sharing Hub

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

© ISO 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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

© ISO 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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.

Documents
Document Sharing Hub

© ISO 2011 – All rights reserved

Full document details: BS ISO 28002:2011

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.

© ISO 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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.

Documents
Document Sharing Hub

© ISO 2011 – All rights reserved

Full document details: BS ISO 28002:2011

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

© ISO 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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]

© ISO 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011

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.

Documents
Document Sharing Hub
© ISO 2011 – All rights reserved
Full document details: BS ISO 28002:2011

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.

© ISO 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 28002:2011