STANDARDS
Australia

AS/NZS 5050:2010

Business continuity—Managing disruption-related risk

STANDARD

AS/NZS

STANDARDS
NEW ZEALAND
PAEREWA AOTEAROA

AS/NZS 5050:2010

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee OB-007, Risk Management. It was approved on behalf of the Council of Standards Australia on 14 May 2010 and on behalf of the Council of Standards New Zealand on 21 May 2010.
This Standard was published on 28 June 2010.

The following are represented on Committee OB-007:

Australian Computer Society
Australian Council of Trade Unions
Dairy Companies Association of New Zealand
Department of Education and Early Childhood Development Victoria
Emergency Management Australia
Engineers Australia
Environmental Risk Management Authority New Zealand
Financial Services Institute of Australasia
Institution of Professional Engineers New Zealand
International Association of Emergency Managers
La Trobe University
Law Society of New South Wales
Massey University
Minerals Council of Australia
Ministry of Economic Development, New Zealand
New Zealand Society for Risk Management
Risk Management Institution of Australasia
Safety Institute of Australia
Society for Risk Analysis, Australia and New Zealand Regional
The Institute of Internal Auditors, Australia
The University of New South Wales
University of Canterbury, New Zealand
Westpool

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.saiglobal.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 09013.

AS/NZS 5050:2010

Australian/New Zealand Standard™

Business continuity—Managing disruption-related risk

First published as AS/NZS 5050:2010.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6140

ISBN 978 0 7337 9615 9

PREFACE

This Standard was prepared by Standards Australia/Standards New Zealand Committee OB-007, Risk Management to assist organizations maintain continuity of their business through effective management of disruption-related risk. This will thereby enhance an organization's resilience and can create strategic and tactical advantage in uncertain and volatile environments.

The approach to managing disruption-related risk described in this Standard (which incorporates concepts often described as 'Business Continuity Management' or 'BCM') is through application of AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines*. Particular emphasis is given to disruptive events of such scale as to otherwise be beyond the capability of an organization's normal management system to cope with.

Managing this type of risk effectively requires a deep understanding of the organization's objectives, its operating environment and its dependencies.

The provisions of this Standard should be an integral part of the organization's plan for risk management. They will help reduce the occurrence and scale of events that could cause disruption as well as equipping the organization with the capacity to—

(a) stabilize any disruptive effects as soon as possible;

(b) continue and/or quickly resume those operations that are most critical to the organization's objectives;

(c) expedite a return to normal operations and a full recovery;

(d) capitalize on any opportunities created by the event; and

(e) assume additional risk with confidence.

The term 'informative' has been used in this Standard to define the application of the appendix to which it applies. An 'informative' appendix is only for information and guidance.

CONTENTS

Page

FOREWORD.................... 4

SECTION 1 SCOPE AND GENERAL
- 1.1 SCOPE 8
- 1.2 REFERENCED DOCUMENTS 8
- 1.3 DEFINITIONS 8

SECTION 2 PRINCIPLES.................... 16

SECTION 3 FRAMEWORK
- 3.1 GENERAL 18
- 3.2 MANDATE AND COMMITMENT.................... 18
- 3.3 DESIGN 19
- 3.4 IMPLEMENTATION.................... 20
- 3.5 MONITORING AND REVIEW OF THE FRAMEWORK 21
- 3.6 CONTINUAL IMPROVEMENT OF THE FRAMEWORK.................... 21

SECTION 4 THE PROCESS
- 4.1 GENERAL 22
- 4.2 ESTABLISHING THE CONTEXT.................... 22
- 4.3 RISK ASSESSMENT 24
- 4.4 RISK TREATMENT.................... 29
- 4.5 COMMUNICATION AND CONSULTATION 35
- 4.6 MONITORING AND REVIEW.................... 36
- 4.7 RECORDING AND DOCUMENTATION.................... 37

SECTION 5 VERIFICATION 38

APPENDIX A ATTRIBUTES OF EFFECTIVE MANAGEMENT OF DISRUPTION-RELATED RISK 46

FOREWORD

All organizations must deal with change in the environments in which they operate. This may relate to changing stakeholder expectations, new strategies adopted by competitors, emerging technologies, changes in staff, availability of finance and the requirements of new legislation. Change is a constant and is best dealt with proactively rather than reactively.

To maintain business continuity, which is a core obligation of good governance, organizations must therefore anticipate and adapt to such changes to avoid either abrupt or progressive failure.

Ensuring business continuity requires a variety of conventional management techniques such as strategic and business planning, continual development of products and services, retaining and acquiring customers, recruiting new staff, raising finance, acquiring technologies and constant attention to quality and efficiency.

However, ensuring business continuity also requires effective management of the organization's risks, including the risks that arise from the possibility of disruptive events. Managing this particular risk to business continuity is the focus of this Standard.

AS/NZS ISO 31000

AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines* is a globally accepted standard for managing all forms of risk.

It advocates that all risks should be managed in an integrated way, supported by an effective framework that sets policy, demonstrates commitment, provides resources, allocates responsibilities and constantly checks progress. It articulates principles for managing risk and also describes the same generic process for managing risks that, since AS/NZS 4360, *Risk management*, was first published in 1995, has been applied by organizations of all types in Australia and New Zealand.

The interrelationship of these elements of AS/NZS ISO 31000 (principles, framework and process) is illustrated in Figure 1.

AS/NZS 5050:2010

This Standard explains how to apply AS/NZS ISO 31000:2009 to disruption-related risks. It includes detailed guidance particular to the features of these risks and to the risk management framework through which they are managed.

The Standard therefore includes a methodology for determining how disruption can affect the continuity of the organization's business and the likelihood of those effects being experienced. This requires a deep understanding of the operating environment as well as a detailed grasp of the organization's objectives and risks. Particular attention is given to those activities, resources, processes and dependencies that are most critical.

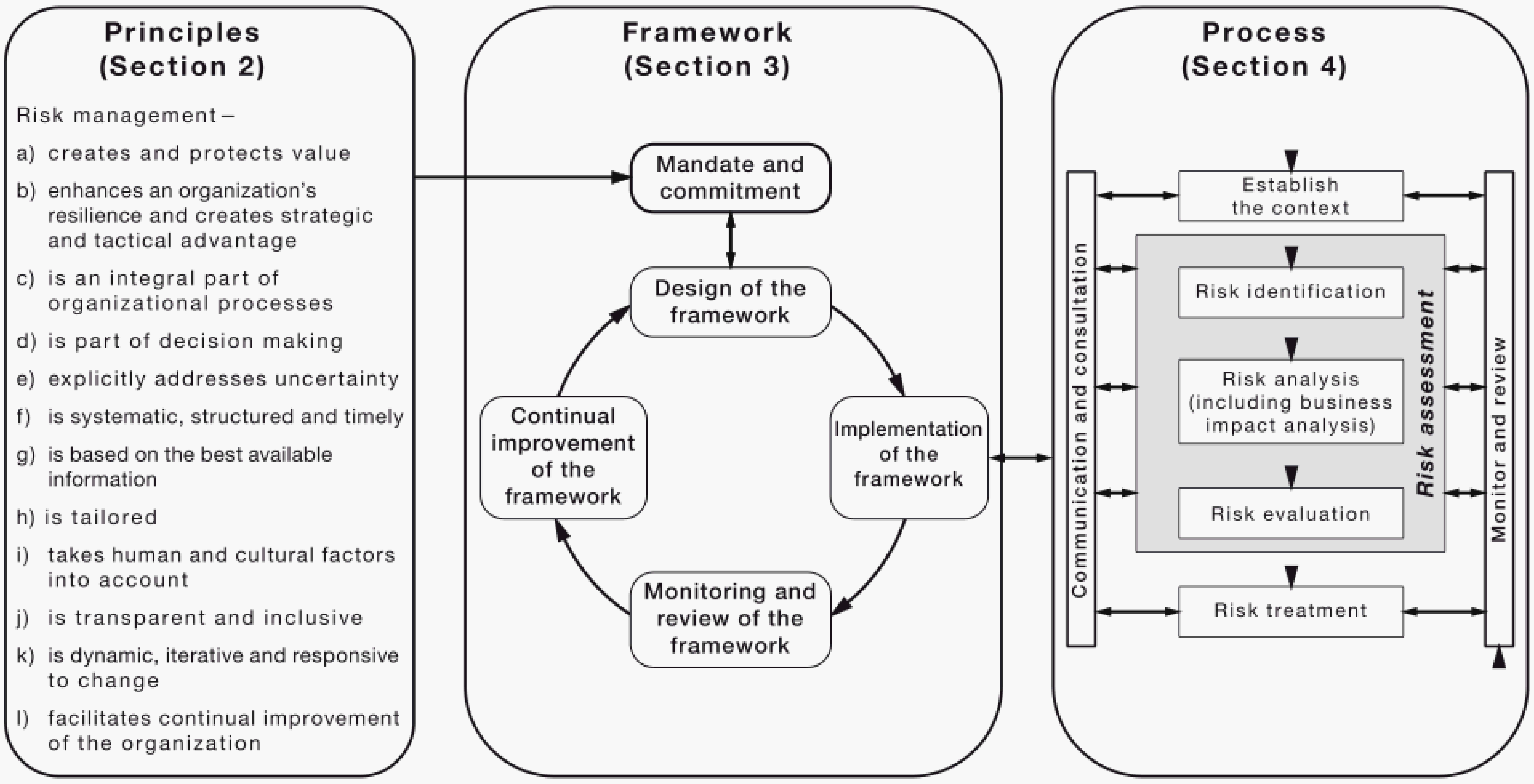

Principles
(Section 2)
Risk management –
a) creates and protects value
b) enhances an organization's resilience and creates strategic and tactical advantage
c) is an integral part of organizational processes
d) is part of decision making
e) explicitly addresses uncertainty
f) is systematic, structured and timely
g) is based on the best available information
h) is tailored
i) takes human and cultural factors into account
j) is transparent and inclusive
k) is dynamic, iterative and responsive to change
l) facilitates continual improvement of the organization
Framework
(Section 3)
Mandate and commitment
Design of the framework
Implementation of the framework
Monitoring and review of the framework
Continual improvement of the framework
Process
(Section 4)
Establish the context
Risk identification
Risk analysis (including business impact analysis)
Risk evaluation
Risk assessment
Risk treatment
Communication and consultation
Monitor and review

FIGURE 1 PRINCIPLES, FRAMEWORK AND PROCESS

The Standard recognizes that some potentially disruptive events may exceed, for some time anyway, the capacity of routine management methods and structures. It therefore explains how to prepare for this by building contingent capacity into the management framework and preparing contingency plans. This allows the organization to quickly change the mode of operations to help ensure business continuity despite occurrence of a potentially disruptive event. Such contingent capacity and plans enable management to quickly focus on stabilizing the situation and maintaining or resuming the most critical functions while still working in a planned way towards eventual restoration of routine operations and full achievement of objectives.

Unlike other guidelines and standards in Australia, New Zealand and elsewhere in the world that address disruption-related risk, AS/NZS 5050 does not limit its consideration of risk treatments to those that only apply once a potentially disruptive event has occurred. It also emphasises that ensuring business continuity in an efficient manner requires consideration of treatments that will reduce the occurrence and scale of events that could cause disruption. Such treatments should be part of the mix of risk treatments because the generally preferable path is not to be disrupted.

Even so, disruptions can sometimes create opportunities. The Standard advocates watching for and being in a position to exploit such possibilities. It also reminds organizations that the cumulative effect of small events, as well as large events can either cause or contribute to the severity of disruption—again emphasising the importance of deep and systematic thinking.

This Standard adopts the defined expressions of AS/NZS ISO 31000 and ISO Guide 73:2009 *Risk management—Vocabulary*. AS/NZS 5050 also uses expressions and language that have become familiar to those who work in this field where this is logical, and consistent with plain English. Together with a few additional definitions, this document standardizes the language used by those managing this type of risk and those managing other risks. This is particularly important if organizations are to succeed in the very important goal of an integrated approach to management of all types of risk.

The Standard includes a Section (5) for those organizations that wish to, or are required to, demonstrate formally that their framework and processes for managing disruption-related risk are able to meet the characteristics of management systems as described in ISO Guide 72[1]. Section 5 does not introduce any additional or different requirements for managing risk.

Figure 2 provides a sense of the relationships between the several areas of focus for managing disruption-related risk.

Before an event, there are opportunities to implement proactive controls that can make potentially disruptive events less frequent or severe, as well as making preparations for contingent controls that are activated once an event commences. These latter controls are aimed at reducing the scale and effects of disruption, returning to routine operations and a full recovery as soon as possible and seizing any opportunities that may arise.

The pre-event preparations include regular maintenance and exercising of the contingency plans and contingent capabilities that enable the organization to respond to the event in a practical and effective way, and transition back to routine management in a planned and controlled manner.

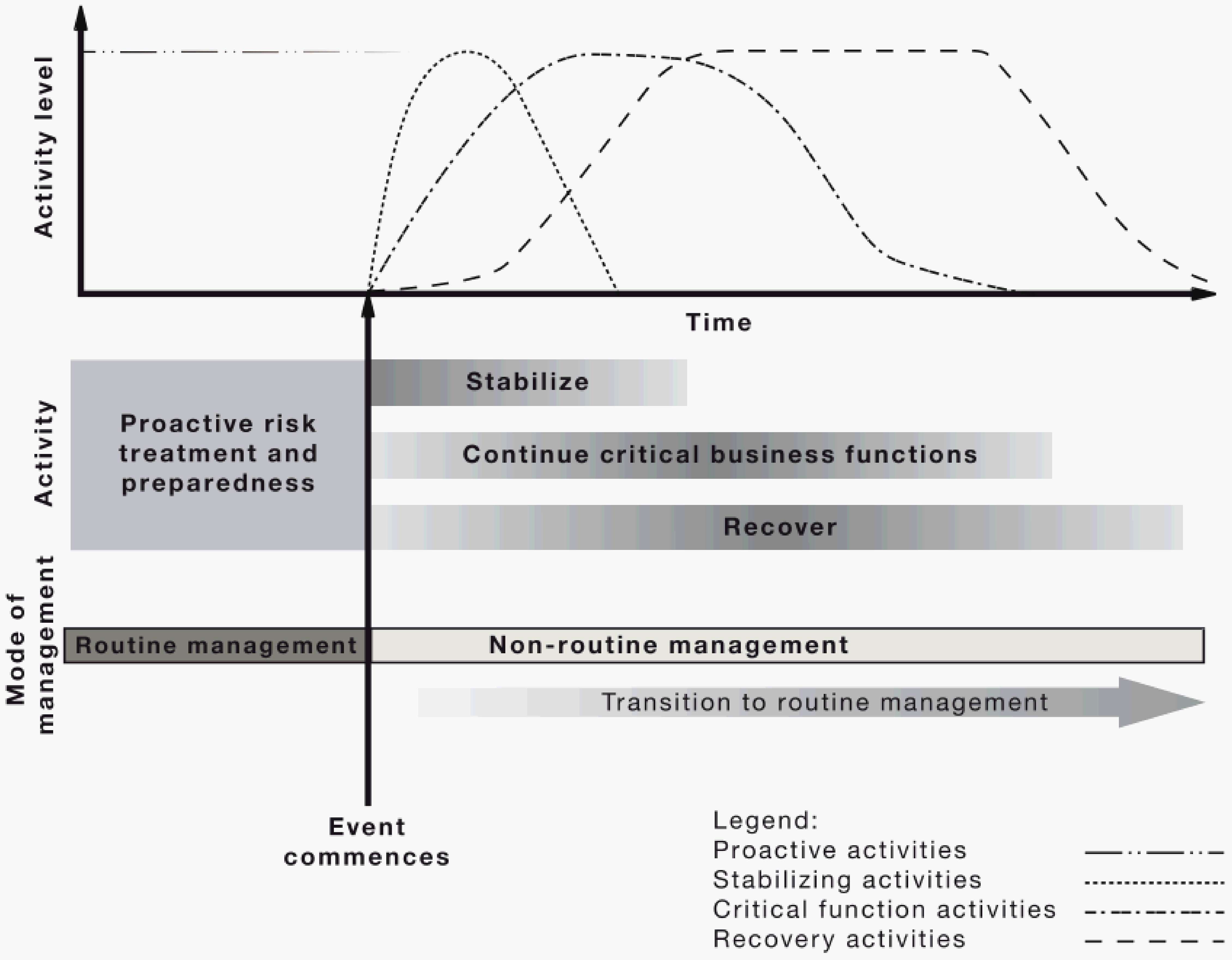


FIGURE 2 RELATIONSHIP OF TREATMENTS FOR DISRUPTION-RELATED RISK

---

[1] ISO Guide 72:2001, *Guidelines for the justification and development of management system standards.*

Other Benefits Of Managing Disruption-Related Risk Effectively

In contributing to maintaining business continuity, managing disruption-related risk also helps organizations to—

(a) demonstrate to internal and external stakeholders, their dependability and good governance;

(b) better understand their own business—sometimes thereby revealing opportunities to improve efficiency, governance and treatment of other risks;

(c) protect and advance brand value;

(d) protect the customer base and market share;

(e) have the confidence to accept further risk; and

(f) remain compliant with relevant legislative or other obligations.

The process of assessing and treating disruption-related risk can in itself contribute to or improve the adaptive capacity of the organization (i.e. its resilience). This occurs through—

(i) increasing awareness of the potential for disruption;

(ii) developing general skills as well as specific capacities which facilitate operating in a non-standard mode; while

(iii) maintaining a strong focus on objectives and critical activities.

STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Australian/New Zealand Standard
Business continuity—Managing disruption-related risk

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE

The Standard describes the application of the principles, framework and process for risk management, as set out in AS/NZS ISO 31000:2009, to disruption-related risk. Managing such risk effectively will help maintain continuity of an organization's business[2]. The approach has drawn on, but of necessity goes beyond, many of the concepts that in the past may have been described as 'Business Continuity Management' or 'BCM'.

The Standard also includes, in Section 5, a schedule of requirements for those organizations seeking or required to demonstrate that their framework and processes for managing disruption-related risk are able to meet the characteristics of management systems as described in ISO Guide 72.

As is the case with AS/NZS ISO 31000, this Standard is applicable to all forms of organization[3].

1.2 REFERENCED DOCUMENTS

The following documents have been referenced in this Standard.

AS/NZS ISO	
9000	Quality management systems—Fundamentals and vocabulary
31000	Risk Management—Principles and guidelines
ISO	
Guide 72	Guidelines for the justification and development of management system standards
Guide 73	Risk management—Vocabulary

1.3 DEFINITIONS

For the purpose of this Standard, the following definitions apply.

1.3.1 Activation

Process whereby all or a portion of a plan is put into effect.

1.3.2 Assurance

Process involving monitoring and review that increases confidence and likelihood that planned objectives will be achieved.

1.3.3 Audit

Process of systematic review against pre-determined criteria.

---

[2] 'Business' refers to the structure, processes and systems that organizations deploy to achieve their objectives.

[3] An 'organization' is any entity with objectives.

NOTES:

1 Whether conducted by internal or external sources, the independence of an audit is determined by the status of the engaging party.

2 The result of an audit will be an assessment against the initial criteria and it will usually provide suggestions for system improvements based on what the auditors have observed.

1.3.4 Business impact analysis (BIA)

Detailed risk analysis that examines the nature and extent of disruptions and the likelihood of the resulting consequences.

NOTE: May include consideration of the organization's business functions, people, processes, infrastructure, resources, information, interdependencies and the nature and extent of capability loss over time.

1.3.5 Business function

Single process or combination of processes contributing to a final definable output or objective.

NOTES:

1 A business function may be a single structural unit of the organization, or may require activity across several structural units.

2 A single structural unit may have responsibility for one or more business functions.

3 A function may be performed by an outsourced or third party provider.

4 May also be referred to as 'business activity'.

1.3.6 Capability

Ability and capacity of people, functions, processes and/or infrastructure to undertake required actions or activities.

1.3.7 Communication and consultation[4]

Continual and iterative processes that an organization conducts to provide, share or obtain information, and engage in dialogue with stakeholders regarding the management of disruption-related risk.

Consultation is a process which impacts on a decision through influence rather than power: an input to decision-making, not joint decision-making.

NOTES:

1 The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of disruption-related risk.

2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a course of action.

1.3.8 Contingency plan

Any plan of action that allows an organization to respond to events should they occur.

NOTES:

1 This includes all plans that deal with stabilization, continuity of critical business functions and recovery.

2 Some types of contingency plans may have been described by terms such as 'business continuity plan' and 'disaster recovery plan'.

1.3.9 Contingent capability

Supplementary resources provided specifically to enable an organization to respond to events should they occur.

NOTE: May be required to make a contingency plan viable.

---

[4] Adapted from ISO Guide 73:2009, *Risk Management—Vocabulary,* definition 3.21.

1.3.10 Control[5]

Measure that is modifying risk.

NOTES:

1 Controls include any process, policy, device, practice, or other actions which modify risk.

2 Controls may not always exert the intended or assumed modifying effect.

1.3.11 Consequence[6]

Outcome of an event affecting objectives.

NOTES:

1 An event can lead to a range of consequences.

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

3 Consequences can be expressed qualitatively or quantitatively.

4 Initial consequences can escalate through knock-on effects.

1.3.12 Crisis

Situation that is beyond the capacity of normal management structures and processes to deal with effectively.

NOTE: A crisis may require significant diversion of management time, attention and resources away from normal, routine operations to respond to the situation.

1.3.13 Critical business function

A business function or part thereof identified as essential for survival of the organization and achievement of its critical objectives.

NOTE: A business function which has the effect of protecting critical interests of the community or another stakeholder to which a duty is owed, may qualify as a critical business function

1.3.14 Critical objectives

Objectives that must be achieved during a period of disruption.

NOTE: Critical objectives may reflect the requirements of external stakeholders.

1.3.15 Disruption-related risk

Risk arising from the possibility of disruptive events.

1.3.16 Establishing the context[7]

Defining the external and internal parameters to be taken into account when managing disruption-related risk and setting the scope and risk criteria for the BCM policy.

1.3.17 Event[8]

Occurrence or change of a particular set of circumstances.

NOTES:

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

2 An event can consist of something not happening.

3 An event can sometimes be referred to as an ‘incident’ or ‘accident’.

4 An event without consequences may also be referred to as a ‘near miss’, ‘incident’, ‘near hit’, or ‘close call’.

---

[5] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.8.1.1.

[6] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.6.1.3.

[7] Adapted from ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.3.1.

[8] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.5.1.3.

1.3.18 External context[9]

External environment in which the organization seeks to achieve its objectives.

NOTE: External context can include—

(a) the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; key drivers and trends having impact on the objectives of the organization; and

(b) relationships with, and perceptions and values of external stakeholders.

1.3.19 Infrastructure

Physical assets and technologies that support an organization.

NOTES:

1 This includes installations, utilities, plant, facilities, structures, installations and technology controlled or used by an organization.

2 For communities, this may include the built environment.

1.3.20 Internal context[10]

Internal environment in which the organization seeks to achieve its objectives.

NOTE: Internal context can include—

(a) governance, organizational structure, roles and accountabilities;

(b) policies, objectives, and the strategies that are in place to achieve them;

(c) the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

(d) information systems, information flows and decision-making processes (both formal and informal);

(e) relationships with, and perceptions and values of, internal stakeholders;

(f) the organization's culture;

(g) standards, guidelines and models adopted by the organization; and

(h) form and extent of contractual relationships.

1.3.21 Likelihood[11]

Chance of something happening.

NOTES:

1 This Standard uses the word 'likelihood' 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).

2 The term 'likelihood' does not have a direct equivalent in some languages; instead, the equivalent of the term 'probability' is often used. However, in English, 'probability' is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, 'likelihood' is used with the intent that it should have the same broad interpretation as the term 'probability' has in many languages other than English.

---

[9] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.3.1.1.

[10] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.3.1.2.

[11] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.6.1.1.

1.3.22 Maximum acceptable outage (MAO)

Maximum period of time that an organization can tolerate the disruption of a critical business function.

NOTES:

1 Disruption may include both the discontinuance of an activity or the inability to perform it to an acceptable quality or with sufficient reliability.

2 Sometimes known as 'maximum tolerable outage' or 'maximum tolerable period of disruption'.

1.3.23 Monitoring[12]

Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

NOTE: Monitoring can be applied to the framework, systems, processes and controls associated with managing disruption-related risk.

1.3.24 Mutual aid

Formalized and documented reciprocal arrangements between two or more organizations providing for unilateral, bilateral or multilateral assistance in specified circumstances.

1.3.25 Recovery

Actions taken following the commencement of a disruptive event to return the organization to routine management.

NOTE: The organization may choose to recover to the pre-disruption state or to a different state.

1.3.26 Recovery Time Estimate (RTE)

Estimated period of time required to restore a particular level of functionality after taking into account any uncertainties.

NOTE: The period is measured from the commencement of the restoration activity and not from the commencement of the disruptive event.

1.3.27 Resilience[13]

Adaptive capacity of an organization in a complex and changing environment.

NOTE: Resilience is a relative expression describing one outcome of the organization's risk management activity. It is not a process, system or framework or other single element of an organization.

1.3.28 Review[14]

Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

NOTE: Review can be applied to a risk management framework, risk management process, risk or control.

---

[12] ISO Guide 73:2009, *Risk management—Vocabulary*, definition 3.8.2.1.

[13] Adapted from ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.8.1.7.

[14] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.8.2.2.

1.3.29 Risk[15]

Effect of uncertainty on objectives.

NOTES:

1 An effect is a deviation from the expected, it may be positive and/or negative.

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

3 Risk is often characterized by reference to potential events and consequences, or a combination of these.

4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

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

1.3.30 Risk analysis[16]

Process to comprehend the nature of risk and to determine the level of risk.

NOTES:

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

2 Risk analysis includes risk estimation.

1.3.31 Risk assessment[17]

Overall process of risk identification, risk analysis and risk evaluation.

1.3.32 Risk criteria[18]

Terms of reference against which the significance of a risk is evaluated.

NOTES:

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

2 Risk criteria can be derived from standards, laws, policies and other requirements.

1.3.33 Risk evaluation[19]

Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

NOTE: Risk evaluation assists in the decision about risk treatment.

1.3.34 Risk identification[20]

Process of finding, recognizing and describing risks.

NOTES:

1 Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.

1.3.35 Risk management[21]

Coordinated activities to direct and control an organization with regard to risk.

---

[15] ISO Guide 73:2009, *Risk management—Vocabulary*, definition 1.1.

[16] ISO Guide 73:2009, *Risk management—Vocabulary*, definition 3.6.1.

[17] ISO Guide 73:2009, *Risk management—Vocabulary*, definition 3.4.1.

[18] ISO Guide 73:2009, *Risk management—Vocabulary*, definition 3.3.1.3.

[19] ISO Guide 73:2009, *Risk management—Vocabulary*, definition 3.7.1.

[20] ISO Guide 73:2009, *Risk management—Vocabulary*, definition 3.5.1.

[21] ISO Guide 73:2009, *Risk management—Vocabulary*, definition 2.1.

1.3.36 Risk management framework

Set of components that provides the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

NOTES:

1 The foundations include the policy, objectives, mandate and commitment to manage risk.

2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

1.3.37 Risk register[22]

Record of information about identified risks.

NOTE: The term 'risk log' is sometimes used instead of 'risk register'.

1.3.38 Risk source[23]

Element which alone or in combination has the intrinsic potential to give rise to risk.

NOTE: A risk source can be tangible or intangible.

1.3.39 Risk treatment[24]

Process to modify risk.

NOTES:

1 Risk treatment can involve—

   (a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

   (b) taking or increasing risk in order to pursue an opportunity;

   (c) removing the risk source;

   (d) changing the likelihood;

   (e) changing the consequences;

   (f) sharing the risk with another party or parties (including contracts and risk financing); and

   (g) retaining the risk by informed decision.

2 Risk treatments that deal with negative consequences are sometimes referred to as 'risk mitigation', 'risk elimination', 'risk prevention' and 'risk reduction'.

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

1.3.40 Stabilization

Activities undertaken to limit deterioration, particularly early in a disruptive event.

1.3.41 Stakeholder[25]

Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

NOTE: A decision maker can be a stakeholder.

---

[22] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.8.2.4.

[23] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.8.2.4.

[24] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.8.1.

[25] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.2.1.1.

1.3.42 Through chain

End-to-end chain through which value is created, realised or transferred, encompassing the inputs, activities and outputs of the supply, process and distribution chains, including information, knowledge, resource and financial flows.

1.3.43 Top management[26]

Person or group of people who directs and controls an organization at the highest level.

1.3.44 Vulnerability[27]

Intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.

---

[26] AS/NZS ISO 9000:2006, *Quality management systems—Fundamentals and vocabulary*.

[27] ISO Guide 73:2009, *Risk Management—Vocabulary*, definition 3.6.1.6.

SECTION 2 PRINCIPLES

The principles of effective risk management given in AS/NZS ISO 31000:2009 form the basis for the following list of principles that are particularly applicable to the management of disruption-related risk. To manage such risk effectively, an organization should adopt and apply the principles below.

(a) Risk management creates and protects value.

It contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

(b) Risk management enhances an organization's resilience and creates strategic and tactical advantage.

The process for managing disruption-related risk involves anticipating rapid change, operating in non-routine modes and adapting to a changing environment within the context of the organization's objectives. The experience of doing this enhances the organization's adaptive capacity.

(c) Risk management is an integral part of all organizational processes.

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

(d) Risk management is part of decision-making.

Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

(e) Risk management explicitly addresses uncertainty.

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

(f) Risk management is systematic, structured and timely.

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

(g) Risk management is based on the best available information.

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

(h) Risk management is tailored.

Risk management is aligned with the organization's external and internal context and risk profile.

(i) Risk management takes human and cultural factors into account.

Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

(j) Risk management is transparent and inclusive.

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

(k) Risk management is dynamic, iterative and responsive to change.

Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

(l) Risk management facilitates continual improvement of the organization.

Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

NOTE: Appendix A provides further advice for organizations wishing to manage risk more effectively.

SECTION 3 FRAMEWORK

3.1 GENERAL

The framework provides the foundations, structures and capabilities to enable the risk management process to be applied and ensure its consistent application.

The elements of the framework and their interrelationships are set out in Figure 3.

To enable the organization to manage disruption-related risk effectively, the risk management framework should have within it additional attributes specific to disruption-related risk, as specified in this Section.

Accordingly, the framework will include elements that reflect the need to operate in both routine and non-routine modes to help ensure business continuity.

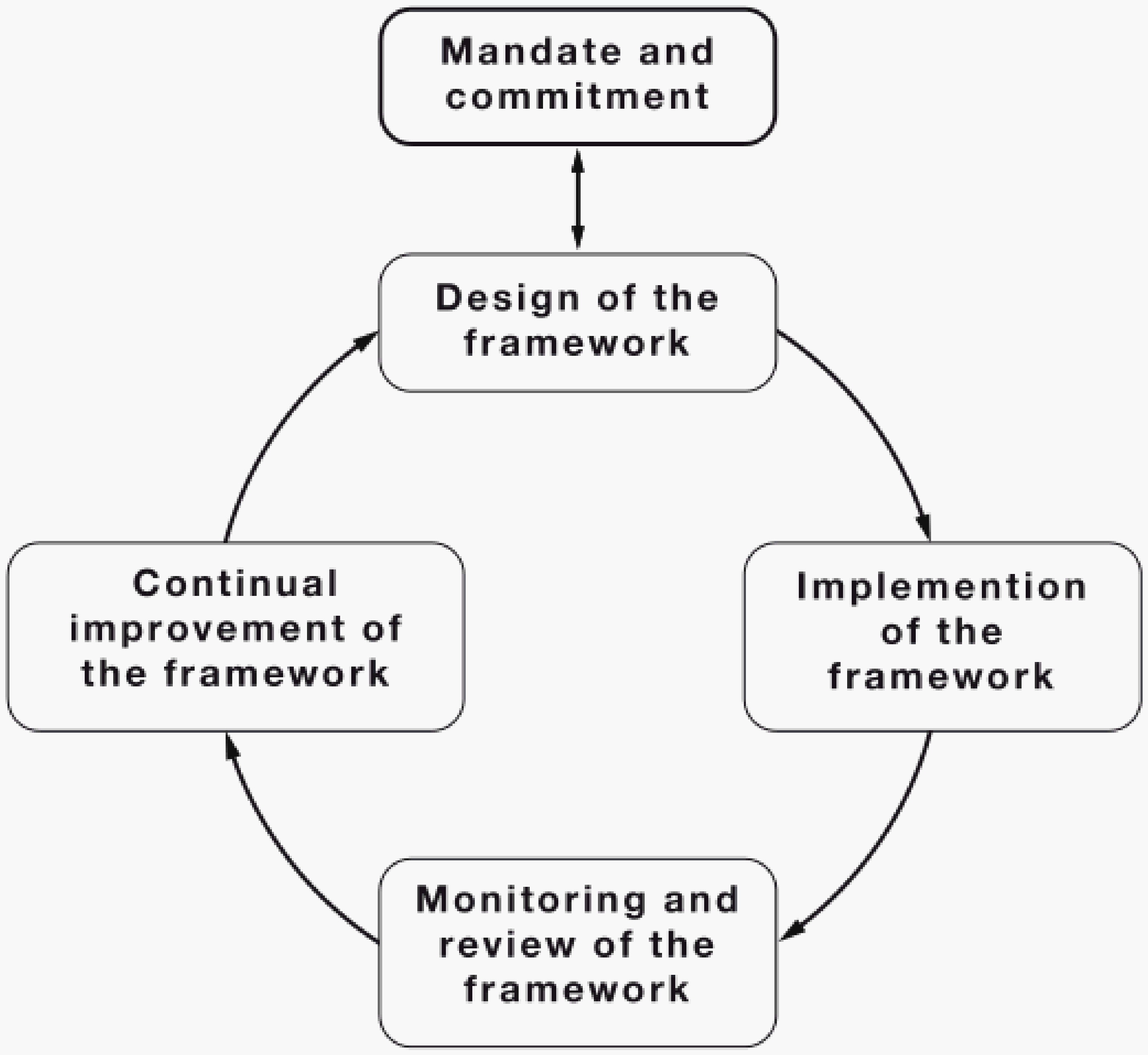

Mandate and commitment
Design of the framework
Implemention of the framework
Monitoring and review of the framework
Continual improvement of the framework

FIGURE 3 RELATIONSHIPS BETWEEN THE COMPONENTS OF THE FRAMEWORK FOR MANAGING DISRUPTION-RELATED RISK

3.2 MANDATE AND COMMITMENT

Ensuring business continuity requires strong and sustained commitment by management at all levels to the management of disruption-related risk.

Management should—

(a) define and endorse the organization’s policy for managing this type of risk;

(b) ensure that the organization’s culture and risk management policies are aligned;

(c) determine risk management performance indicators that align with performance indicators of the organization;

(d) ensure legal and regulatory compliance;

(e) assign accountabilities and responsibilities at appropriate levels within the organization;

(f) ensure that the necessary resources are allocated to the management of this type of risk;

(g) generate awareness by communicating the benefits of business continuity to relevant stakeholders; and

(h) ensure that the framework for managing this type of risk continues to remain appropriate.

3.3 DESIGN

3.3.1 The organization and its context

The framework for managing disruption-related risk should take into account the external and internal context of the organization taking particular account of future volatility and changing interdependencies.

The external factors include, but are not limited to—

(a) the social and cultural, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

(b) key drivers and trends having impact on the objectives of the organization; and

(c) the form and nature of relationships including interdependencies with, and perceptions and therefore values of, external stakeholders.

The internal factors include, but are not limited to—

(i) governance arrangements including policies, structures, roles and accountabilities and decision-making processes (both formal and informal);

(ii) objectives, and the strategies that are in place to achieve them;

(iii) capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

(iv) information systems, reporting and other information flows;

(v) the organization's culture; and

(vi) standards and guidelines adopted by the organization.

For each of the above set of factors, past experience, the present situation and potential future circumstances should be considered.

3.3.2 Establishing the policy

The policy should clearly state the organization's objectives for, and commitment to, the management of disruption-related risk and typically addresses—

(a) the organization's rationale for ensuring business continuity;

(b) links between the organization's objectives and policies and this policy;

(c) accountabilities and responsibilities for managing this type of risk;

(d) commitment to make the necessary resources available to assist those accountable and responsible for managing this type of risk; and

(e) the way in which performance against this policy will be measured and reported; and

(f) commitment to review and improve the policy and framework periodically and in response to an event or change in circumstances.

The policy, which preferably will form part of the organization's overall policy about managing risk, should be communicated appropriately.

3.3.3 Accountability

The organization should ensure that there is accountability, authority and appropriate competence for all aspects of managing disruption-related risk. This can be facilitated by—

(a) identifying risk owners that have the accountability and authority to manage this type of risk;

(b) identifying who is accountable for the development, implementation and maintenance of the framework for managing this type of risk;

(c) identifying other responsibilities of people at all levels in the organization who contribute to business continuity;

(d) establishing performance measurement and external and/or internal reporting and escalation processes; and

(e) ensuring appropriate recognition of accountability and performance.

3.3.4 Integration

Managing disruption-related risk should be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. Therefore, the process for managing this type of risk should be part of, and not separate from, those organizational processes. In particular, it should be integrated into the policy development, business and strategic planning and review, and change management processes.

The organization should plan how the management of this type of risk will be integrated in all of the organization's practices and processes.

3.3.5 Resources

The organization should allocate appropriate resources to each step in the process for managing disruption-related risk. This should consider—

(a) funding;

(b) people, skills, experience and competence;

(c) tools, methods and supporting infrastructure;

(d) information and knowledge management systems; and

(e) the possibility of having to operate in non-routine modes.

3.3.6 Communication and reporting

The organization's framework for managing disruption-related risk should include communication and reporting arrangements. This will assist in—

(a) building awareness, confidence and understanding;

(b) meeting regulatory and other legal requirements; and

(c) exchanging information with stakeholders.

3.4 IMPLEMENTATION

In implementing or enhancing a framework for managing disruption-related risk, the organization should—

(a) define the appropriate timing and strategy;

(b) integrate the framework across existing organizational arrangements;

(c) comply with legal and regulatory requirements;

(d) hold information and training sessions;

(e) delegate or amend accountabilities and responsibilities; and

(f) ensure that the process for managing risk (see Section 4) is applied throughout the organization for this type of risk.

3.5 MONITORING AND REVIEW OF THE FRAMEWORK

To ensure the framework remains effective and appropriate, the organization should—

(a) measure the performance of the framework against indicators, which are periodically reviewed for appropriateness;

(b) periodically measure progress against, and deviation from, the risk management plan; periodically review whether the framework, policy and plan are still appropriate, given the organization's external and internal context;

(c) report on how well the risk management policy is being followed; and

(d) assess the effectiveness of the management of disruption-related risk using the criteria given in Appendix A.

3.6 CONTINUAL IMPROVEMENT OF THE FRAMEWORK

Based on results of monitoring and reviews, decisions should be made on how the framework can be improved.

SECTION 4 THE PROCESS

4.1 GENERAL

The process for managing disruption-related risk should be—

(a) an integral part of management; and

(b) tailored to the business processes of the organization.

It comprises the activities described in Clauses 4.2 to 4.5 supported by those described in Clauses 4.6 and 4.7 at each step as shown in Figure 4.

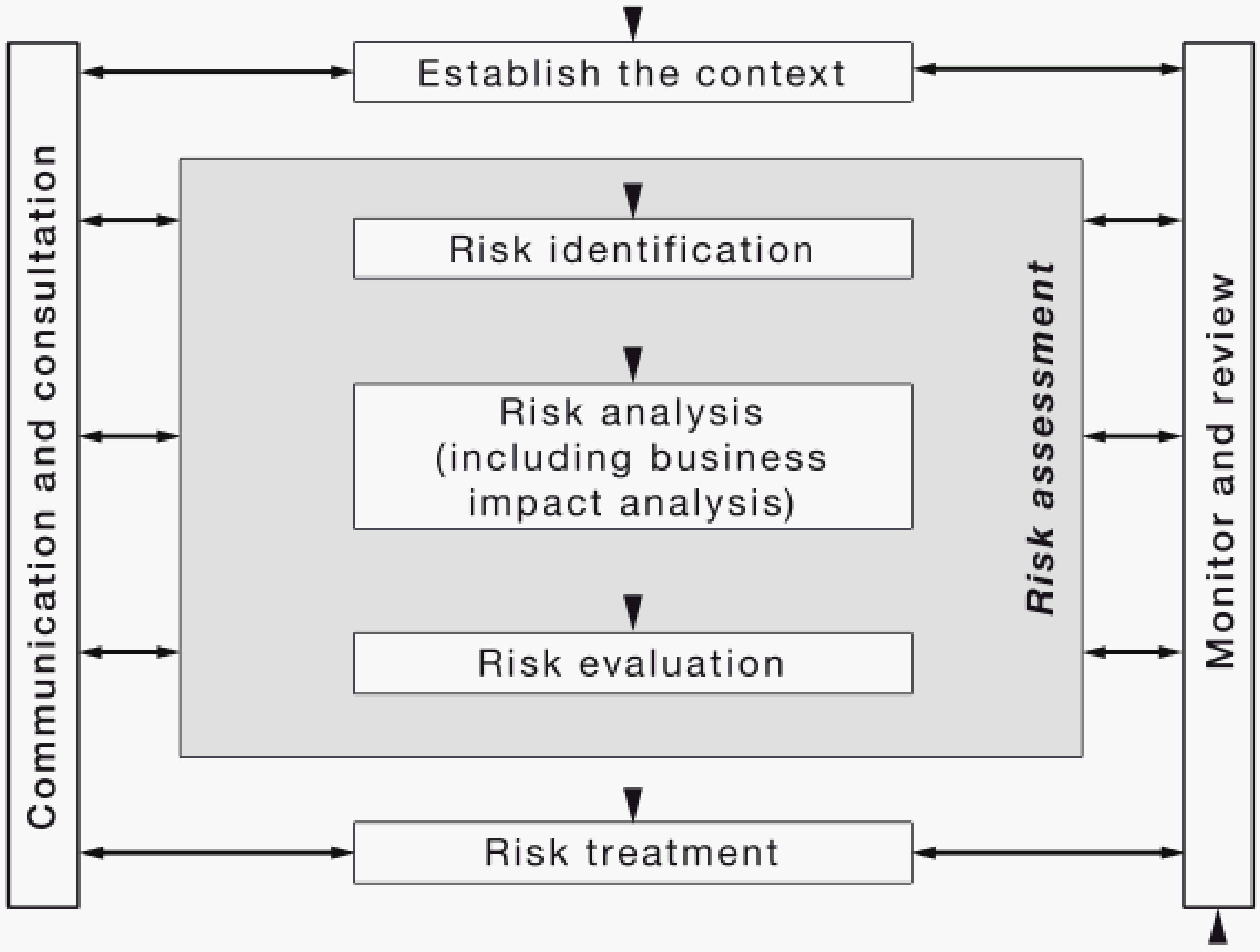


FIGURE 4 PROCESS FOR MANAGING DISRUPTION-RELATED RISK

4.2 ESTABLISHING THE CONTEXT

4.2.1 General

In establishing the context, the organization—

(a) articulates its objectives, including those concerned with business continuity;

(b) identifies its stakeholders and their objectives;

(c) defines the external and internal factors that create the uncertainty that gives rise to risk;

(d) sets risk criteria; and

(e) defines the scope and purpose of the particular risk management activity.

While many of these parameters are similar to those considered in the design of the framework (see Clause 3.3.1), when establishing the context for the risk management process, they need to be considered in greater detail including how they relate to managing disruption-related risk.

4.2.2 Objectives

The objectives of the organization include its explicit and implicit goals, values and imperatives. The objectives of some organizations may be set by statute.

4.2.3 Establishing the external context

The external context characterizes pertinent features of the external environment in which the organization seeks to achieve its objectives. The external context can include, but is not limited to—

(a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

(b) external infrastructure on which the organization depends including market, utilities, suppliers, and logistics;

(c) key external drivers and trends having impact on the objectives of the organization; and

(d) relationships with, and perceptions, values and objectives of external stakeholders.

4.2.4 Establishing the internal context

The internal context characterizes pertinent features of the internal environment in which the organization seeks to achieve its objectives. This can include, but is not limited to—

(a) governance arrangements including policies, structures, roles and accountabilities and decision making processes (both formal and informal);

(b) the strategies that are in place to achieve objectives;

(c) capabilities, understood in terms of resources and knowledge (e.g. time, people, processes and systems);

(d) physical assets, technologies and internal infrastructure;

(e) capital, financial arrangements and income streams;

(f) information systems, reporting and other information flows;

(g) the organization's culture; and

(h) standards and guidelines adopted by the organization.

4.2.5 Defining risk criteria

The organization should define criteria to be used to evaluate the significance of disruption-related risk. These criteria should be consistent with the organization's general risk criteria, its values and objectives. Some criteria can be imposed by, or derived from, legal and regulatory requirements. Risk criteria should be consistent with the organization's risk management policy (see Clause 4.3.2), be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered should include—

(a) the nature and types of consequences that can occur and how they will be measured; how likelihood will be defined;

(b) the timeframe(s) of the likelihood and/or consequence(s);

(c) how the level of risk is to be determined;

(d) the views of stakeholders; and

(e) the level at which risk becomes acceptable or tolerable.

4.2.6 Establishing the purpose, scope and structure of the particular risk management activity

The scope and purpose of a particular risk management activity must be clear to ensure that it is appropriate to the organization's needs for business continuity and its objectives.

This includes, but is not limited to—

(a) defining the goals and objectives of the activity;

(b) defining responsibilities for elements of the activity;

(c) defining the scope, depth and breadth of the activity, including specific inclusions and exclusions;

(d) defining the risk assessment structure and methodologies; and

(e) identifying and specifying the decisions that have to be made.

4.3 RISK ASSESSMENT

4.3.1 Overview

Risk assessment refers to the process of identification, analysis and evaluation of disruption-related risks. See Figure 4.

It has been common in management of disruption-related risk to characterize aspects of these processes as 'business impact analysis'. In this Standard, this expression has been reserved to describe that part of the risk analysis process that examines in detail the mechanisms, sequences, timeframes and extent of disruptive consequences that require treatment and are likely to exceed the capacity of routine management methods and tools.

4.3.2 Risk identification

The aim of this step is to generate a comprehensive list of risks based on those events that might disrupt the organization; whether these events may enhance, prevent, degrade, accelerate or delay the achievement of objectives.

The identification of disruption-related risk should consider the sources of risk, their areas of impacts, potential types of events, their causes and types of consequence. Information such as existing risk registers should be considered and may facilitate the identification of additional disruption-related risks.

Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis. Identification should include risks whether or not their source is under the control of the organization. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.

The organization should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks.

4.3.3 Risk analysis

4.3.3.1 *General*

Risk analysis involves developing an understanding of disruption-related risk. It provides an input to risk evaluation and to decisions on whether these risks need to be treated and on the most appropriate risk treatment strategies and methods. In many cases, it will need to be conducted in an iterative manner with the initial analysis permitting an initial evaluation of the risks and selection of a general treatment strategy and a subsequent more granular analysis of particular aspects of the risk being used to inform the detailed selection and design of particular risk treatments within the general strategy.

It involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that can affect consequences and likelihood including the presence (or not) and effectiveness of existing controls should be identified.

An event can vary in scale and so have multiple and varying consequences thus affecting business continuity in several ways. The way in which consequences and their likelihoods are expressed and the way in which they are combined to determine a level of risk should be consistent with the risk criteria. Consequences can include direct and indirect as well as tangible and intangible impacts on business continuity.

Analysis of disruption-related risk is usually best approached in two stages with the first stage being conducted at sufficient precision to allow evaluation of the risks and thereafter, development of a broad treatment strategy. Depending on the quality of the organization's existing risk assessment, this may be able to be conducted using information from the risk register.

The second stage, which in this Standard is called 'Business Impact Analysis', is aimed at building a very detailed understanding of those disruptive consequences that require treatment and as such are likely exceed routine methods of management or require additional management capability.

4.3.3.2 *Initial risk analysis*

The initial risk analysis should include building a clear understanding of—

(a) the business functions and processes;

(b) the magnitude of the contribution of each of these functions and processes to the organization's objectives;

(c) the location and distribution of infrastructure and resources;

(d) the vulnerabilities of the systems, physical structures and locations in which business activity occurs (having regard to the likely effect of any existing controls);

(e) the principal types of internal and external dependency including (but not limited to) infrastructure, utilities, human expertise, knowledge and experience, suppliers and customers; and

(f) other factors critical to the organization's business activity.

One or more risk analysis tools (such as process mapping, event or fault tree analysis) should be selected for the initial analysis. Modelling may be required to understand some aspects of internal and external dependencies.

This information can be used to develop a small number of representative scenarios that could lead to disruption. For each of these scenarios, using information from the risk identification about how and when disruptions might occur, preliminary estimates should be developed of—

(a) the time required to restore the most important disrupted activities and the effect, in terms of the selected risk criteria—such as impact on revenue, impact on reputation and market share on the organization's objectives; and

(b) the extent to which restoration activities can be accomplished by the current capability and responsibilities of the management team having regard to other obligations to maintain other operations that have not been disrupted.

This information enables a preliminary evaluation of the risk (refer Clause 4.3.4) and the development of initial risk treatment plans (refer Clause 4.4.3). Where the preliminary analysis does not provide sufficiently reliable information to inform risk treatment or if after initial treatment the residual risk is not tolerable, then a more detailed study called a business impact analysis is warranted.

4.3.3.3 *Business Impact Analysis (BIA)*

BIA provides detailed insight into the extent, timeframes and mechanisms of disruptive consequences and their likelihoods. This confirms which business functions are critical and informs the detailed design of further treatment, should this be required.

In some cases, due to the complexity of the organization, it will be necessary to limit the analysis to a representative selection of scenarios involving disruption, from the frequent to the very unlikely.

Those having particular knowledge of the business functions under examination should be consulted. This may include those who are responsible for specific processes within the business function, those responsible for other interdependent functions and with other key stakeholders.

Overall the BIA should reveal—

(a) processes, capabilities, infrastructure and other resources (including those of external dependencies) which, if disrupted, would prevent the organization achieving its critical objectives and whether in each case this is influenced by when the disruption occurs or the duration of the disruption;

(b) the level of vulnerability of processes, capabilities, infrastructure and other resources to disruption; and

(c) the organization's priorities and opportunities given the particulars of the analysis.

The key steps in conducting the BIA are summarized in Figure 5 and guidance is given below.

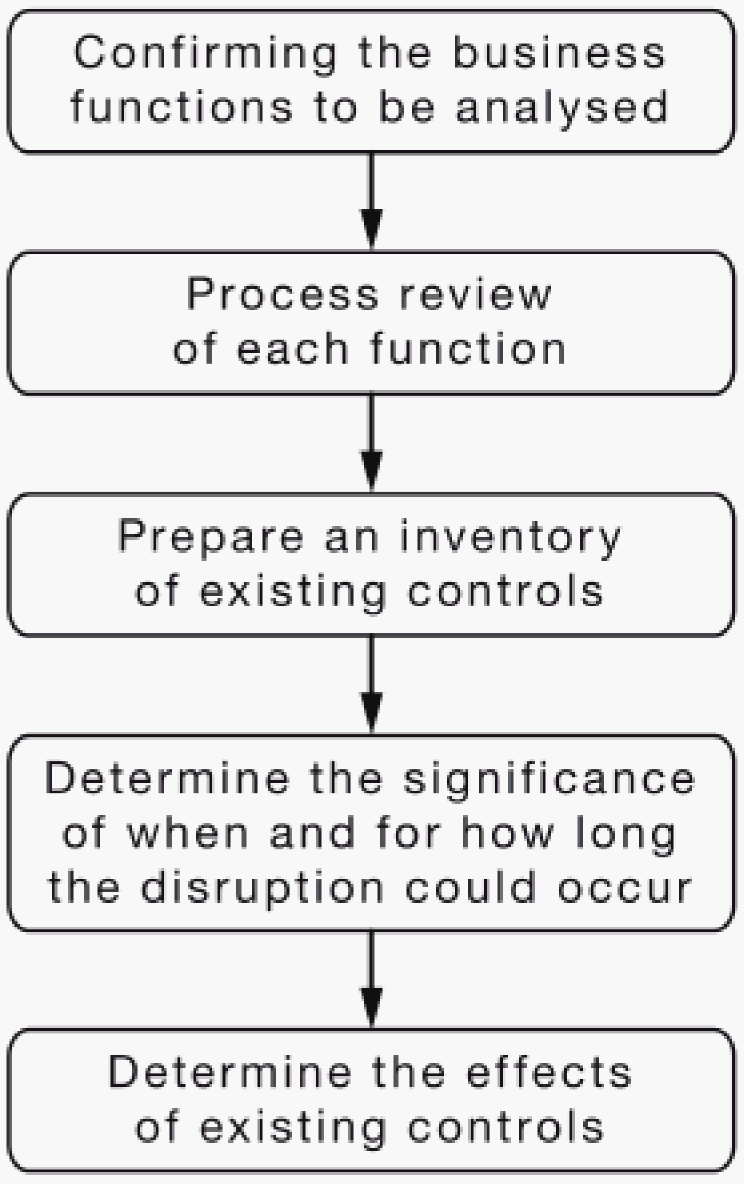

Confirming the business functions to be analysed
Process review of each function
Prepare an inventory of existing controls
Determine the significance of when and for how long the disruption could occur
Determine the effects of existing controls

FIGURE 5 BUSINESS IMPACT ANALYSIS

Step 1—Confirming the business functions to be analysed

The previous context setting and risk analysis steps will have indentified the business functions of interest. BIA should commence by seeking top management’s confirmation of this.

This step may result in some previously nominated business functions being removed from further consideration and additional business functions being added to the BIA.

Step 2—Process review of each function

This step involves the detailed analysis of each function and their associated processes and interdependencies to identify the disruption impacts. This will include the *in situ* examination of each process and their dependencies, and when the process must be available.

Step 3—Prepare an inventory of existing controls

This involves undertaking a review of the current arrangements including preparedness, existing strategies, plans, processes, resources and capabilities. These may include:

(a) Work-arounds including rescheduling or alternative processes.

(b) Redundant capacity.

(c) Outsourcing.

(d) Supporting plans and arrangements.

(e) Availability and reliability of supporting laws and arrangements.

Included in the inventory of controls are the controls in external organizations on which there is a high level of reliance.

The effect of existing controls is considered in Step 5.

Step 4—Determine the significance of when and for how long disruption could occur

The significance of disruption of a business function depends on its duration and timing when compared with the maximum acceptable outage (MAO) for that function. The MAO should be derived from the risk criteria and the initial risk analysis but may be further refined as a result of this step. The MAO should be confirmed or varied by top management.

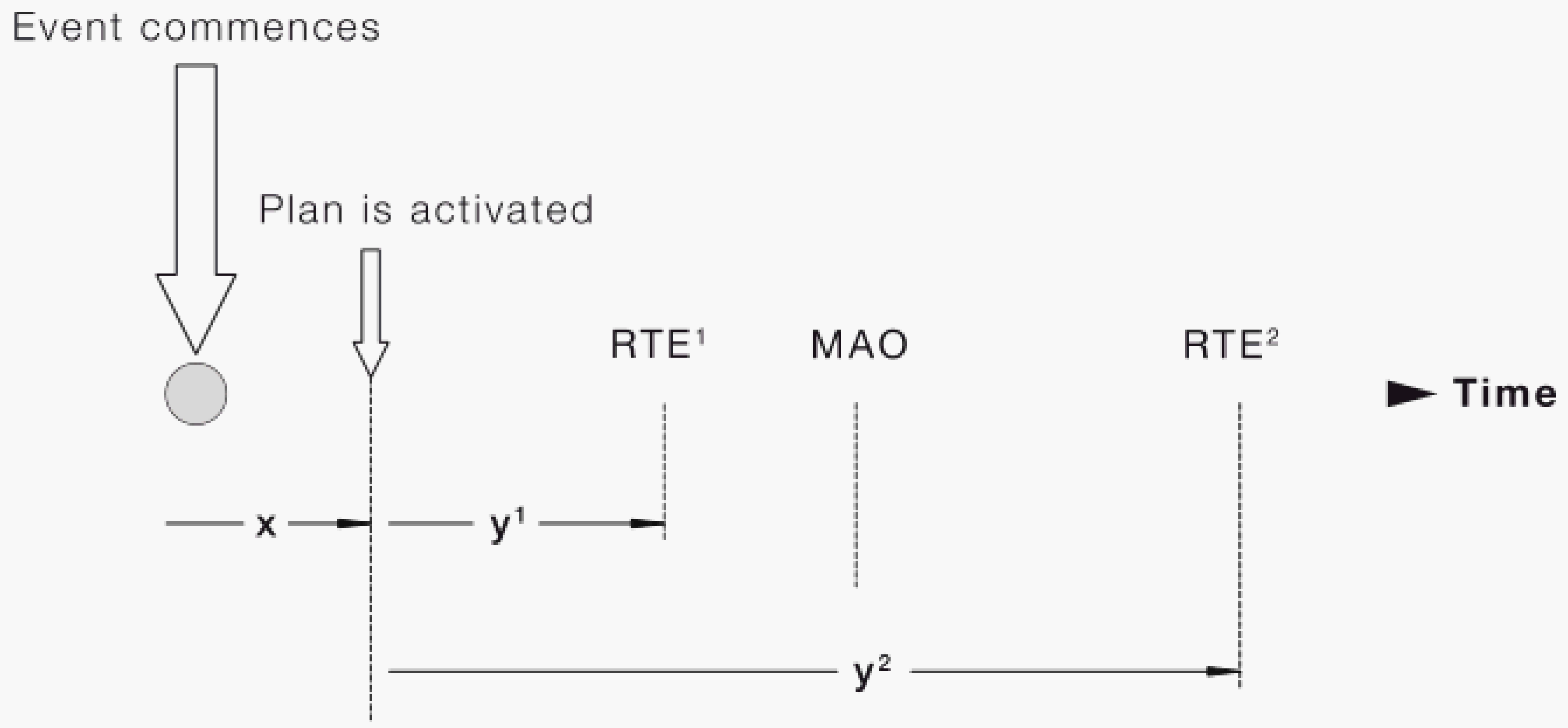
The time intervals used when considering duration should be relevant to the context and the function being analysed (e.g. minutes, hours or days). Consideration of the timing of disruption should take account of the operational cycle of that function, for example, the time of day, date or season when the disruption occurs.

Step 5—Determine the effect of existing controls

The effect of existing controls should be determined, including the length of time required for such controls to come into service. This may involve obtaining advice from internal services and external providers about the anticipated timeframes involved for them to restore a service or resume supply once they have been asked to do so.

The resulting recovery time estimate (such as RTE^1 or RTE^2 in Figure 6) will therefore take into account the time required to activate any plan (x on Figure 6) together with time required to implement it (such as y^1 or y^2 on Figure 6).

Step 5 should take account of any uncertainties around estimates of time.



NOTE: y^1 and y^2 have been sometimes referred to as 'recovery time objectives'.

FIGURE 6 DETERMINING THE CASE FOR TREATMENT

4.3.3.4 *Consolidating the risk analysis*

The outputs from the initial risk analysis and the BIA should be consolidated so that the overall consequences and associated likelihoods of disruption-related risk are recorded in terms consistent with the risk criteria previously established to enable evaluation and risk treatment if required.

4.3.4 Risk evaluation

The purpose of risk evaluation is to assist in making decisions about which elements of disruption-related risk (including existing controls) need treatment and the priority for implementation. This should be based on the outcomes of the risk analysis.

Risk evaluation involves comparing the level of risk found during the analysis process (including the BIA) with risk criteria established when the context was considered.

Decisions should take account of the wider context of the disruption-related risk including the impact on other parties and legal requirements.

In some circumstances, the risk evaluation can lead to a decision to undertake additional analysis of business impacts. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls.

4.4 RISK TREATMENT

4.4.1 General

4.4.1.1 *Risk treatment options*

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify controls. The selection process involves balancing the costs and the efforts of implementation against the benefits derived; which should also take into account the organization's wider obligations.

Risk treatment therefore involves a cyclical process of—

(a) selecting one or more risk treatment options;

(b) deciding whether, either alone or in combination with other risk treatments or controls, residual risk levels would become tolerable;

(c) if not tolerable, generating a new risk treatment or set of risk treatments; and

(d) assessing the effectiveness, costs and benefits of the treatment(s).

Some types of risk treatment can provide other benefits to the organization and for that reason, it may be valid in some circumstances to further treat the risk even though other treatments will have made it tolerable.

In general terms, risk treatment options will involve one or more of the following actions—all of which should be considered:

(i) Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.

(ii) Removing the risk source.

(iii) Changing likelihood.

(iv) Changing consequences.

(v) Sharing the risk with another party or parties (including contracts and risk financing).

(vi) Retaining the risk by informed decision.

4.4.1.2 *Treating disruption-related risk*

Treatment of disruption-related risk should be considered in terms of each of the organization's risk criteria. For example, while sharing risk via insurance may be an effective treatment of the financial consequences of disruption, it may not adequately treat reputational consequences or prevent long term loss of market share—both of which can prove very difficult to adequately insure—or, necessarily, allow statutory organizations to continue to fulfil their mandate.

For disruption-related risks, treatment options fall into the following two broad categories, both of which should be considered:

(a) Proactive approaches involving prevention and protection measures which will influence the likelihood and scale of potentially disruptive events.

(b) Those which, if a potentially disruptive event occurs, either preclude or minimize any impact on business continuity and, therefore achievement of objectives ('contingency plans' and 'contingent capability'). Contingency plans and contingent capability involving some combination of—

  (i) elimination or modification of the organization's vulnerability to potentially disruptive events by building contingent capability (for example, provision of redundant or backup capacity, improvements or modification of processes, diversification of particular supplier dependencies, insurance or other risk financing arrangements); and

  (ii) development of contingency plans (reflecting the supporting capability) that can be activated after an event occurs in order to variously stabilize the situation, restore or continue critical functions and expedite restoration of normality. Such plans, which are discussed in greater detail below, may include communication with stakeholders, workarounds, and temporary reallocation of management responsibilities. Associated with these plans will often be a requirement for development of supporting capacity (for example establishing a alternative capability that can assume all or part of particular functions) and always a maintenance (see 4.4.4) and exercise (see 4.4.5) regime.

As noted above, an iterative approach may be needed for the selection of treatments. Initially a broad treatment strategy should be selected for the risks that are shown by the evaluation of the preliminary analysis to require treatment. This will include finding the right combination of treatments in each of the categories (a) and (b) above.

4.4.1.3 *Selecting treatments*

When selecting treatments the organization should also take the following into account:

(a) Regulations, government policy, industry standards, social and community obligations, and organizational policies.

(b) Existing controls.

(c) Development, implementation and ongoing costs (including those associated with maintenance and exercising of contingency plans).

(d) Risk arising from the risk treatment process.

(e) Any new risks arising from the new controls.

(f) Capability of the organization to implement the treatments.

(g) Validity of assumptions about the performance of external organizations (for example, emergency services, alternative suppliers and stakeholders) and the reliability of contingent agreements (for example mutual aid or priority supply contracts).

(h) Ancillary costs and benefits (tangible and intangible).

As part of developing risk treatments, the organization should—

(i) review existing controls for adequacy and effectiveness; and

(ii) examine the linkages between the activities to stabilize the situation, restore or continue critical functions and expedite restoration of normality.

4.4.2 Proactive risk treatment

The purpose of this form of risk treatment is to modify the scale and likelihood of events that could cause disruption. These include—

(a) implementing preventive controls in the form of operating practices, inspections, procedures and devices that make it less likely that a disruptive event will occur; and

(b) implementing protective controls which, if the preventive controls fail, limit the scale of the potentially disruptive event by reducing its intensity, duration or spread or the vulnerability of the organization's assets to the effects.

This may also involve seeking the implementation of such controls by external parties on which the organization has high levels of reliance.

These forms of risk treatment should be considered first and in preference to those described in Clause 4.4.3. They should always be part of the overall strategy for treating disruption-related risk.

4.4.3 Contingency plans and contingent capability

4.4.3.1 *General*

The purpose of this form of treatment is to improve the organization's ability to respond quickly and optimally to events should they occur.

Contingency plans may take many forms but will address—

(a) stabilization;

(b) continuing critical functions; and

(c) recovery.

Contingency plans need to be developed in the context of the organizational capacity on which they rely. Therefore, to make a plan viable or more efficient it may be necessary to also develop additional contingent capability such as providing back up facilities, built-in redundancy or alternative supply arrangements to those normally relied upon.

Some plans may be suitable for implementation by the normal management system. Others may require deployment of either an additional or re-configured management structure (sometimes called a 'crisis management team') together with associated changes in delegations. The decision to move to a non-routine mode of management should take account of—

(i) the scale, scope and speed of decision-making that may be required;

(ii) the intensity and likely duration of non-routine management activity;

(iii) the limits of normal delegated authority;

(iv) the capabilities of the management team;

(v) the possibility that the disruptive event may have injured or isolated members of the management team; and

(vi) the possibility that the organization may have to maintain some business-as-usual operations while responding to a disruptive event elsewhere in the organization.

Deployment and operation of such special management arrangements, which may have multiple levels—each with appropriate escalation triggers—will also require careful planning with the plan being part of the suite of contingency plans. The plan should ensure that in a disruptive event, those with authority to implement or escalate to non-routine management arrangements are kept well informed of the situation to assist them in their decision-making. The planning should have regard to the need to preserve good governance when operating in non-routine mode.

All contingency plans should include criteria for activation and the logistical arrangements for activation. These arrangements should contemplate the possibility that the primary or preferred method of activation could be rendered unusable by the disruptive event and so should include alternatives.

Plans and/or their content can become out of date, so regular and specific maintenance should be an intrinsic part of the plan. When plans are activated, those involved will often be required to operate in non-routine roles. Regular exercise of plans is therefore necessary to maintain familiarity and this also should be a part of the plan.

4.4.3.2 *General requirements for contingency plans*

4.4.3.2.1 *Purpose*

The purpose of plans is to aid decision-making during a potentially disruptive event by—

(a) clearly articulating the overall objective;

(b) providing priorities and guidance on actions;

(c) providing information that is required quickly but cannot be easily obtained;

(d) providing an alternative or modified management structure if the normal one is not suitable for dealing with a disruptive event;

(e) preserving good governance during a disruptive event; and

(f) enhancing identification and realization of opportunities.

4.4.3.2.2 *Responsiveness*

Plans should reflect the ability of the management team to respond to non-routine circumstances and should be—

(a) fit for purpose;

(b) tailored to the organization and its objectives;

(c) as simple and succinct as possible;

(d) understandable;

(e) realistic and achievable;

(f) consistent with and linked to other plans;

(g) viable in the absence of particular individuals;

(h) up-to-date;

(i) in an easily usable and accessible format, within the constraints of confidentiality; and

(j) wherever possible, aligned with other plans (such as the coordinated incident management structure commonly used by public agencies for dealing with large scale disruptions or emergencies and the contingency plans of a dependent customer) with which they may need to interface.

4.4.3.2.3 *Contents*

Plans should contain—

(a) version, date and issuing authority;

(b) purpose and scope;

(c) activation and stand down criteria including an applicability check at the time of activation to ensure the plan is relevant to the particulars of the actual situation;

(d) cross-reference and linkages to other plans;

(e) roles, accountabilities and responsibilities;

(f) process descriptions;

(g) details for accessing resources;

(h) communication and consultation requirements; and

(i) schedules of critical information including contact lists, maps and plans.

The outcomes of good planning are improved organizational resilience and the demonstration of readiness.

Clauses 4.4.3.3 to 4.4.3.5 provide detailed requirements for the three major forms of treatments in a contingency plan.

4.4.3.3 *Stabilization*

Stabilization treatments involve activities undertaken to limit further deterioration, particularly early in a disruptive event. This will include—

(a) acting to preserve life;

(b) preventing the spread of further harm;

(c) countering the source of harm;

(d) removing critical resources from harm;

(e) communicating with stakeholders;

(f) salvaging to prevent further deterioration; and

(g) stopping unnecessary expenditure.

Such plans may require provision of contingent capacity such as emergency equipment.

4.4.3.4 *Continuing critical functions*

This form of treatment involves either early restoration, or ensuring continuation, of the organization’s critical functions (as identified in the business impact analysis) following a potentially disruptive event. It involves planning to take specific actions for each critical function or group of functions.

To ensure the plans are viable, this may also require installing or developing further capability and resources in anticipation of a disruptive event (e.g. establishing spare or backup capacity for later deployment).

Treatment may necessitate—

(a) preparing fresh delegations of authorities for individuals who are to assume new roles;

(b) developing workarounds, alternative work methods, or locations;

(c) deploying alternative information and communications technology infrastructure and associated data and information;

(d) establishing contingent agreements with current suppliers or customers;

(e) adopting alternative logistics (including, possibly, suppliers and customers);

(f) sourcing critical equipment or materials by salvage from the affected location or transfer from another;

(g) redeploying or accessing additional human resources;

(h) hibernating, such as temporarily reducing or ceasing non-critical activities.

If it is not cost effective to continue a critical activity in particular circumstances, a decision may be taken to discontinue it and to liquidate the residual assets.

4.4.3.5 *Recovery*

The overall aim of recovery treatments is to return the organization to an acceptable and routine state. This will involve recovering the business to its pre-disruption condition or to another state that takes advantage of opportunities or changed circumstances.

Treatment may necessitate—

(a) confirming or modifying objectives and priorities for recovery;

(b) allocating resources to this form of risk treatment;

(c) identifying the activities to achieve the recovery objectives;

(d) taking opportunities by—

  (i) re-designing work methods and layout;

  (ii) replacing obsolete equipment and systems;

  (iii) re-engineering processes to enhance quality and efficiency;

  (iv) offering different services and products;

  (v) renegotiating supply, logistics and customer agreements; and

  (vi) withdrawing from selected markets, locations, or industries;

(e) planning implementation of the contingent activities including—

  (i) costing and funding (including managing any insurance claim);

  (ii) tendering and purchase;

  (iii) obtaining consents and approvals;

  (iv) risk assessment; and

  (v) project management;

(f) communicating and consulting with stakeholders;

(g) establishing activities to allow the organization to learn from the disruptive event and from the successes and failures of the treatment activities; and

(h) commissioning and resumption of normal operations.

4.4.4 Maintain the plans

Contingency plans should be routinely maintained so that they are up-to-date and the organization is ready to deploy them. The scope and frequency of maintenance activity should be defined when plans are developed, and should address the following:

(a) *Knowledge, skills and understanding* The effectiveness of some aspects of plans will depend on certain individuals or those occupying specific positions having particular knowledge, skills and understanding at the time the plan is deployed. This requires routine training and testing. Individuals appointed to new or changed positions should be briefed on their roles and responsibilities and provided with the necessary knowledge and competencies.

(b) *Resources* Contingent resources on which plans rely require ongoing monitoring and maintenance, particularly where these are not used routinely but need to be available should a disruptive event occur. Maintenance may require upgrading, replacing or repairing such resources.

(c) *Currency of information* It is to be expected that some information forming part of contingency plans will become out of date (e.g. contact details) and will require updating. Such information should be specifically identified and subject to an automatic review process. Consideration should be given, where possible, to automate updating of new or revised information (e.g. automatically updating plans with changes to the names of individuals in the organizational chart).

4.4.5 Exercise the plans

Exercising helps ensure that plans will work when deployed. Frequency of exercising should have regard to the complexity of the plans.

The principal types of exercise are—

(a) notification and communications call-out, that involve the activation of key personnel and tests the ability to reach contacts identified within the plan;

(b) seminar, interview, discussion and workshop exercises, that allow individuals to provide information on their responsibilities and capabilities and to share experiences and concerns about responding to disruptive events;

(c) tabletop (or desk top) review using hypothetical disruption scenarios;

(d) walk-through, in the form of a guided discussion to enhance understanding of the components and structures of the plans;

(e) functional exercise or TEWT (tactical exercise without troops), to practise decision-making;

(f) deployment (full scale) exercise, which involves a 'live' activation of plans based on a hypothetical scenario(s), to enhance decision-making and test logistics and contingent resources;

(g) recovery test, which involves either closing down or removing access to key elements of systems or infrastructure and activating contingent capability; and

(h) testing, to confirm operability of contingent capability.

A formal post-exercise review should be planned as an integral part of the exercise process to ascertain the lessons to be learnt and enable improvement. Planning for the review should include determining the manner in which performance is to be assessed and evaluated. Gathering this information may require specific resources.

Participants and rolls played in exercises should take into account the possibility that some members of the organization may not be available to fulfil their designated role at the time of a potentially disruptive event.

4.5 COMMUNICATION AND CONSULTATION

Communication and consultation with external and internal stakeholders should facilitate truthful, relevant, accurate and understandable exchanges of information and should take place during all stages of the process for managing disruption-related risk. This helps ensure that both those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made and have the opportunity to contribute to them.

Communication should be a two-way process so as to confirm that questions, ideas and information have transferred successfully. This requires consideration of the capabilities and experiences of the parties, the form of communication and any factors that might affect 'transmission' and 'receipt' of ideas (e.g. the use of technical language with lay audiences).

Communication and consultation should take into account legitimate needs for confidentiality.

Consultation with stakeholders and others can provide access to relevant information and experience that will assist in the management of disruption-related risk. Consultation should be undertaken in a way that ensures that those being consulted understand the context in which their responses are likely to be applied. They should be given sufficient contextual information, and time, in order to provide considered input.

The views of stakeholders may include judgements about risk based on their perceptions which may reflect personal or organizational values, needs, knowledge, assumptions, concepts and concerns. Such perceptions should be taken into account.

High quality communication and consultation are required because disruption-related risks can involve ambiguity, are often complex and may involve extreme events that are outside normal human experience. Plans for communication and consultation should therefore be developed at an early stage.

Throughout the course of an event, communication that is accurate and authoritative can provide both reassurance and information to stakeholders. Provided that it gains respect for its currency, quality and accuracy, such communication can be an important form of risk treatment for disruptive events. The likely interest and needs of the media during this period should be taken into account in the communications plan.

4.6 MONITORING AND REVIEW

Both monitoring and review should be a planned part of the process for managing disruption-related risk and involve regular checking or surveillance in order to provide assurance of ongoing relevance, readiness and effectiveness.

Monitoring and review can be periodic or ad hoc.

Responsibilities for monitoring and review should be clearly defined.

The organization's monitoring and review processes should be aimed at—

(a) detecting any change in the organization's objectives;

(b) detecting changes in the external and internal context, including changes to risk criteria;

(c) the risk itself which can require revision of risk treatments and priorities;

(d) tracking progress on implementation of risk treatment plans;

(e) ensuring that controls (of both the organization and its key external dependencies), including contingency plans, their maintenance and testing, are effective and efficient in both design and operation;

(f) obtaining further information to improve risk assessment including the business impact analysis;

(g) analysing and learning lessons from potentially disruptive events (including near misses), testing and maintenance activities, and changes, trends, successes and failures; and

(h) identifying emerging disruption-related risks.

Elements of monitoring and review may also be incorporated in the performance measures of individuals with responsibilities for management of disruption-related risk.

As part of its monitoring and review activities, an organization should gain assurance that the framework and process for the management of disruption-related risk are working effectively and within the policy it has set. In particular, the scope of assurance arrangements should include all of the parameters in Appendix A.

To be effective, assurance should comprise a combination of the following activities:

(i) Continuous (or at least frequent) monitoring through routinely measuring or checking particular parameters.

(ii) Line management reviews of disruption-related risks and their treatments; and independent review and audit—using both internal and external audit staff.

The results of monitoring and review should be recorded and externally and internally reported, as appropriate, preferably as part of the organization's routine performance management and assessment arrangements. The results should also be used as an input to the review of the framework for managing disruption-related risk.

4.7 RECORDING AND DOCUMENTATION

4.7.1 General

Recording and documentation should be fit for purpose and current and be protected against loss, inappropriate use or corruption.

4.7.2 Recording the risk management process

Risk management activities should be traceable. Such records also provide the foundation for improvement in methods and tools, as well as in the overall process.

Decisions concerning the creation, content and format of records should take into account—

(a) the organization's needs for continuous learning;

(b) benefits of re-using information for management purposes;

(c) costs and efforts involved in creating and maintaining records;

(d) legal, regulatory and operational needs for records;

(e) method of access, ease of retrieval and storage arrangements;

(f) retention period; and

(g) sensitivity of information.

4.7.3 Contingency plan documentation

The content of contingency plans and information that is needed for implementation of the plans should be—

(a) in a form and method of storage that survives the event and meets any legislative requirements;

(b) classified according to its purpose and importance and based on that purpose; and

(c) readily accessible and useable to those who will require it, within the timeframes assumed in the contingency plans and irrespective of the effects of the event.

The integrity and currency of such information must be protected and assured, as must the method of accessibility.

Sensitive information should be protected against misuse or loss.

Contingency plans should specifically include provisions to capture, as the event progresses, information about the event and about the effect of the plan.

Particular attention should be given to capture, document and preserve information that will be useful for stabilization, continuation of critical functions, recovery, and subsequent review of the foregoing.

SECTION 5 VERIFICATION

Table 5.1 sets outs verifiable requirements for those organizations wishing or required to show that their framework and process for managing disruption-related risk is consistent with requirements of a management system as defined in ISO Guide 72: 2001.

Table 5.1 therefore does not apply to organizations not requiring such verification.

The elements and requirements given in Table 5.1 are in a style and manner that is consistent with ISO Guide 72.

NOTE: Organizations choosing to meet these requirements (and other organizations relying on the fact that they have been met) should not conclude that as a result, all disruption-related risks will be managed effectively. Such assurance is only likely if there is compliance with all aspects of Sections 1–4 of this Standard and if the attributes of the organization's approach to the management of disruption-related risk are consistent with those described in Appendix A.

TABLE 5.1

VERIFICATION REQUIREMENTS FOR ELEMENTS OF THE ORGANIZATION'S MANAGEMENT SYSTEM RELATING TO MANAGEMENT OF DISRUPTION-RELATED RISK

Main subjects	Elements	Component requirement in relation to the framework for managing disruption-related risk	Component requirement in relation to the process for managing disruption-related risk	Component requirement in relation to the treatment of disruption-related risk
1 Policy	1 Policy and principles	The organization has a written policy in accordance with Clause 3.3.2.		
2 Planning	2.1 Identification of needs analysis requirements and analysis of critical issues.	The organization has established the external and internal context when designing its risk management framework in accordance with Clause 3.3.1. This includes any contractual or regulatory requirements.	The organization routinely establishes the external and internal context before conducting risk assessment in accordance with Clauses 4.2.3 and 4.2.4. It conducts risk identification in accordance with Clause 4.3.2.	
	2.2 Selection of significant issues to be addressed		The organization analyses risks as required by Clause 4.3.3, undertaking initial analysis in accordance with Clause 4.3.3.2 and then Business Impact Analysis in accordance with Clause 4.3.3.3 to prioritise risks for attention.	
	2.3 Setting of objectives and targets	The objectives for the management of disruption-related risk are clearly stated in the organization's policy statement in accordance with Clause 3.3.2 and the requirements for the implementation of the framework with timeframes and performance indicators in accordance with Clause 3.4.	Risk criteria are set that allow the organization to evaluate the significance of disruption-related risk in accordance with Clause 4.2.5. The organization defines the objectives of particular risk management in accordance with Clause 4.2.6.	

(continued)

TABLE 5.1 (*continued*)

Main subjects	Elements		Component requirement in relation to the framework for managing disruption-related risk	Component requirement in relation to the process for managing disruption-related risk	Component requirement in relation to the treatment of disruption-related risk
	2.4	Identification of resources	Appropriate resources for the management of disruption-related risk are allocated in accordance with Clause 3.3.5.	When selecting risk treatments, the organization identifies the resources needed to treat disruption-related risk in accordance with Clause 4.4.1.	The organization monitors and maintains the contingent resources that contingency plans rely on in accordance with Clause 4.4.5.
	2.5	Identification of organizational structure, roles, responsibilities and authorities	The organization has ensured that there is accountability, authority and appropriate competence for all aspects of managing disruption-related risk in accordance with Clause 3.3.3.	The responsibility for monitoring and review is clearly defined in accordance with Clause 4.6.	Contingency plans, in accordance with Clause 4.4.3.1, contain clear descriptions of roles, accountabilities and responsibilities.
	2.6	Planning of operational processes	The organization plans how the management of disruption-related risks is integrated into all the organization's practices and processes in accordance with Clause 3.3.4.		
	2.7	Contingency preparedness for foreseeable events			The organization treats the risks from potential disruptive events in accordance with Clause 4.4. It develops proactive forms of risk treatment in accordance with Clause 4.4.2 and contingency plans and contingent capability in accordance with Clause 4.4.3. Contingency plans are maintained as required by Clause 4.4.4 and exercised in accordance with Clause 4.4.5.

(*continued*)

TABLE 5.1 (*continued*)

Main subjects	Elements	Component requirement in relation to the framework for managing disruption-related risk	Component requirement in relation to the process for managing disruption-related risk	Component requirement in relation to the treatment of disruption-related risk
3 Implementation and operation	3.1 Operational control	The organization has implemented a framework for the management of disruption-related risk in accordance with Clause 3.4. The framework and its implementation are monitored and reviewed in accordance with Clause 3.5.		
	3.2 Management of human resources	The organization has allocated human resources including employees, contractors and temporary staff for each step in the process for managing disruption-related risk in accordance with Clause 3.3.5 that includes consideration of skills, experience and competence.		Regular training and testing are provided for those individuals occupying specific positions that require particular knowledge, skills and understanding at the time a contingency plan is deployed in accordance with Clause 4.4.4. Individuals appointed to new or changed positions are briefed on their roles and responsibilities and provided with the necessary knowledge and competencies with respect to contingency plans in accordance with Clause 4.4.4.

(*continued*)

TABLE 5.1 (*continued*)

Main subjects	Elements	Component requirement in relation to the framework for managing disruption-related risk	Component requirement in relation to the process for managing disruption-related risk	Component requirement in relation to the treatment of disruption-related risk
	3.3 Management of other resources	Other resources such as tools, methods, supporting infrastructure, information and knowledge management systems are allocated to each step of the process for managing disruption-related risk in accordance with Clause 3.3.5. The performance of these other resources is monitored and reviewed in accordance with Clause 3.5.	Other resources that are controls are monitored and reviewed as required by Clause 4.6.	Other resources such as operating practices, inspections, procedures and devices that are preventive controls or protective controls are provided in accordance with Clause 4.4.2. Contingent capability to support the implementation of contingency plans is provided in accordance with Clause 4.4.3. These contingent resources are maintained in accordance with Clause 4.4.4.
	3.4 Documentation and its control	The organization's policy for the management of disruption-related risk has been documented in accordance with Clause 3.3.2. The plan for how the organization will integrate the management of disruption-related risk into its practices and processes has been documented in accordance with Clause 3.3.4. Periodically, the organization has monitored and reviewed its policy and plan in accordance with Clause 3.5.	The organization records its risk management process in accordance with Clause 4.7.1.	The organization documents its contingency plans in accordance with Clause 4.7.2.

(*continued*)

TABLE 5.1 (*continued*)

Main subjects	Elements	Component requirement in relation to the framework for managing disruption-related risk	Component requirement in relation to the process for managing disruption-related risk	Component requirement in relation to the treatment of disruption-related risk
	3.5 Communication	The organization has ensured that its policy for the management of disruption-related risk is appropriately communicated in accordance with Clause 3.3.2. The organization's framework for the management of disruption-related risk includes communication and reporting arrangements in accordance with Clause 3.3.6.	Suitable communication and consultation with external and internal stakeholders takes place in accordance with Clause 4.5 during all stages of the process for managing disruption-related risk.	
	3.6 Relationship with suppliers and contractors			Where the performance of suppliers and contractors can give rise to potential disruptions or where their performance is required as part of risk treatment, the organization considers the validity of assumptions about that performance when selecting risk treatments in accordance with Clause 4.4.1. Where suppliers and contractors are expected to provide contingent capability including resources, the organization ensures that that capability and those resources are available when required through the provision of contingent agreement in accordance with Clause 4.4.3.4. The organization ensures that supplier or contractor supplied capabilities and resources are maintained in accordance with Clause 4.4.4.

(*continued*)

TABLE 5.1 (*continued*)

Main subjects		Elements		Component requirement in relation to the framework for managing disruption-related risk	Component requirement in relation to the process for managing disruption-related risk	Component requirement in relation to the treatment of disruption-related risk
4	Performance assessment	4.1	Monitoring and measuring	The organization ensures that the framework for the management of disruption-related risk is monitored and reviewed in accordance with Clause 3.5.	The organization ensures that the process used for the management of disruption-related risk is monitored and reviewed in accordance with Clause 4.6.	The organization plans formal post-exercise reviews to ascertain the lessons to be learnt and to implement improvement in accordance with Clause 4.4.5.
		4.2	Analysing and handling nonconformities	Based on the results of the monitoring and review of the framework for managing disruption-related risk in accordance with Clause 3.5, the organization makes decisions on how the framework can be improved in accordance with Clause 3.6.	Based on the results of the monitoring and review of the process for managing disruption-related risk, the organization makes decisions on how the framework can be improved in accordance with Clause 4.6.	In planning for formal post-exercise reviews, the organization determines the manner in which performance is to be assessed and evaluated in accordance with Clause 4.4.5.
		4.3	System audits	The organization audits the framework for managing disruption-related risk, as part of the monitoring and review activities in accordance with Clause 3.5.		
5	Improvement	5.1	Corrective action	Based on the results of the monitoring and review of the framework for managing disruption-related risk in accordance with Clause 3.5, the organization makes decisions on how the performance of the framework can be continually improved in accordance with Clause 3.6. This involves eliminating the causes of nonconformities.	Based on the results of the monitoring and review of the process for managing disruption-related risk in accordance with Clause 4.6, the organization makes decisions on how the performance of the process can be continually improved. This involves eliminating the causes of nonconformities.	In planning for formal post-exercise reviews, the organization determines the manner in which performance is to be assessed and evaluated in accordance with Clause 4.4.5.

(*continued*)

TABLE 5.1 *(continued)*

Main subjects	Elements	Component requirement in relation to the framework for managing disruption-related risk	Component requirement in relation to the process for managing disruption-related risk	Component requirement in relation to the treatment of disruption-related risk
	5.2 Preventive action	Based on the results of the monitoring and review of the framework for managing disruption-related risk in accordance with Clause 3.5, the organization makes decisions on how the performance of the framework can be continually improved in accordance with Clause 3.6. This includes the mechanism for instigating action to eliminate the causes of nonconformities.	Based on the results of the monitoring and review of the process for managing disruption-related risk in accordance with Clause 4.6, the organization makes decisions on how the performance of the process can be continually improved. This includes the mechanism for instigating action to eliminate the causes of nonconformities.	In planning for formal post-exercise reviews, the organization determines the manner in which performance is to be assessed and evaluated in accordance with Clause 4.4.5. This includes the mechanism for instigating action to eliminate the causes of nonconformities.
	5.3 Continual improvement	Based on the results of the monitoring and review of the framework for managing disruption-related risk in accordance with Clause 3.5, the organization makes decisions on how the framework can be continually improved in accordance with Clause 3.6.	Based on the results of the monitoring and review of the process for managing disruption-related risk, the organization makes decisions on how the framework can be continually improved in accordance with Clause 4.6.	The organization plans and undertakes formal post-exercise reviews to ascertain the lessons to be learnt and to implement improvement in accordance with Clause 4.4.5.
6 Management review	6.1 Management review	The organization periodically conducts a management review of the framework for managing disruption-related risk, as part of the monitoring and review activities in accordance with Clause 3.5.	The organization periodically conducts a management review of the process for managing disruption-related risk, as part of the monitoring and review activities in accordance with Clause 4.6.	

APPENDIX A

ATTRIBUTES OF EFFECTIVE MANAGEMENT OF DISRUPTION-RELATED RISK

(Informative)

A1 GENERAL

This Appendix sets out the attributes of effective management of disruption-related risk, together with tangible indicators for each. All organizations should aim to ensure that their framework for managing this risk delivers these attributes and should measure their performance accordingly.

A2 OUTCOME ATTRIBUTES

Characteristics of outcome attributes are that—

(a) the organization has a current, correct and comprehensive understanding of its disruption-related risks; and

(b) the organization's level of disruption-related risk is within its risk criteria.

A3 PROCESS ATTRIBUTES

A3.1 Continual improvement

An emphasis is placed on continual improvement in management of disruption-related risk through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

This can be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance can be published and communicated. Normally, there will be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.

This performance assessment is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

A3.2 Full accountability for disruption-related risks

Enhanced management of disruption-related risk includes comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. Designated individuals fully accept accountability, are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders.

This can be indicated by all members of an organization being fully aware of the risks, controls and tasks for which they are accountable. Normally, this will be recorded in job/position descriptions, databases or information systems. The definition of risk management roles, accountabilities and responsibilities should be part of all the organization's induction programes.

The organization ensures that those who are accountable are equipped to fulfil that role by providing them with the authority, time, training, resources and skills sufficient to assume their accountabilities.

A3.3 All related decision-making involves consideration of disruption-related risk

All decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of disruption-related risks and the application of risk management process to some appropriate degree.

This can be indicated by records of meetings and decisions to show that explicit discussions on risks took place. In addition, it should be possible to see that all components of the process for the management of disruption-related risk are represented within key processes for decision making in the organization, e.g. for decisions on the allocation of capital, on major projects and on re-structuring and organizational changes. For these reasons, soundly based risk management is seen within the organization as providing the basis for effective governance.

A3.4 Continual communications

Enhanced management of disruption-related risk includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.

This can be indicated by communication with stakeholders as an integral and essential component of risk management. Communication is rightly seen as a two-way process, such that properly informed decisions can be made about the level of risks and the need for risk treatment against properly established and comprehensive risk criteria.

Comprehensive and frequent external and internal reporting on both significant disruption-related risks and on risk management performance contributes substantially to effective governance within an organization.

A3.5 Full intefreation into the organization’s governance structure

Management of disruption-related risk is viewed as central to the organization’s management processes, so that such risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization’s objectives.

This is indicated by managers’ language and important written materials in the organization using the term ‘uncertainty’ in connection with disruption-related risks. This attribute is also normally reflected in the organization’s statements of policy, particularly those relating to risk management. Normally, this attribute would be verified through interviews with managers and through the evidence of their actions and statements.

NOTES

Standards Australia

Standards Australia is an independent company, limited by guarantee, which prepares and publishes most of the voluntary technical and commercial standards used in Australia. These standards are developed through an open process of consultation and consensus, in which all interested parties are invited to participate. Through a Memorandum of Understanding with the Commonwealth government, Standards Australia is recognized as Australia's peak national standards body.

Standards New Zealand

The first national Standards organization was created in New Zealand in 1932. The Standards Council of New Zealand is the national authority responsible for the production of Standards. Standards New Zealand is the trading arm of the Standards Council established under the Standards Act 1988.

Australian/New Zealand Standards

Under a Memorandum of Understanding between Standards Australia and Standards New Zealand, Australian/New Zealand Standards are prepared by committees of experts from industry, governments, consumers and other sectors. The requirements or recommendations contained in published Standards are a consensus of the views of representative interests and also take account of comments received from other sources. They reflect the latest scientific and industry experience. Australian/New Zealand Standards are kept under continuous review after publication and are updated regularly to take account of changing technology.

International Involvement

Standards Australia and Standards New Zealand are responsible for ensuring that the Australian and New Zealand viewpoints are considered in the formulation of international Standards and that the latest international experience is incorporated in national and Joint Standards. This role is vital in assisting local industry to compete in international markets. Both organizations are the national members of ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

Visit our web sites

www.standards.org.au
www.standards.com.au
www.standards.co.nz

ISBN 978 - 0 - 7337 - 9615 - 9

Standards Development
Standards Australia
GPO Box 476
Sydney NSW 2001
Phone: 02 9237 6000
Fax: 02 9237 6010
Email: mail@standards.org.au
Internet: www.standards.org.au

Sales and Distribution
SAI Global
Phone: 13 12 42
Fax: 1300 65 49 49
Email: sales@saiglobal.com

This page has been left intentionally blank.