

COMMITTEE OB-007

DR 09054 CP

(Project ID: 8976)

Combined Postal Ballot/Draft for Public Comment Australian/New Zealand Standard

LIABLE TO ALTERATION—DO NOT USE AS A STANDARD

BEGINNING DATE **3 August 2009**
FOR COMMENT:

CLOSING DATE **21 September 2009**
FOR COMMENT:

Business continuity—Managing disruption-related risk
Part 2: Practice



STANDARDS
Australia



STANDARDS
NEW ZEALAND
PAEREWĀ AOTEAROA

COPYRIGHT

Combined Postal Ballot/ Draft for Public Comment Australian/New Zealand Standard

The committee responsible for the issue of this draft comprised representatives of organizations interested in the subject matter of the proposed Standard. These organizations are listed on the inside back cover.

Comments are invited on the technical content, wording and general arrangement of the draft.

The preferred method for submission of comment is to download the MS Word comment form found at <http://www.standards.com.au/Catalogue/misc/Public Comment Form.doc>. This form also includes instructions and examples of comment submission.

When completing the comment form ensure that the number of this draft, your name and organization (if applicable) is recorded. Please place relevant clause numbers beside each comment.

Editorial matters (i.e. spelling, punctuation, grammar etc.) will be corrected before final publication.

The coordination of the requirements of this draft with those of any related Standards is of particular importance and you are invited to point out any areas where this may be necessary.

Please provide supporting reasons and suggested wording for each comment. Where you consider that specific content is too simplistic, too complex or too detailed please provide an alternative.

If the draft is acceptable without change, an acknowledgment to this effect would be appreciated.

When completed, this form should be returned to the Projects Manager, Andrew McKay via email to Andrew.mckay@standards.org.au.

Normally no acknowledgment of comment is sent. All comments received electronically by the due date will be put before the relevant drafting committee. Because Standards committees operate electronically we cannot guarantee that comments submitted in hard copy will be considered along with those submitted electronically. Where appropriate, changes will be incorporated before the Standard is formally approved.

If you know of other persons or organizations that may wish to comment on this draft Standard, could you please advise them of its availability. Further copies of the draft are available from the SAI Global Customer Service Centre listed below and from our website at <http://www.saiglobal.com/>.

SAI GLOBAL Customer Service Centre

Telephone: 13 12 42

Facsimile: 1300 65 49 49

e-mail: mailto:sales@saiglobal.com

Internet: <http://www.saiglobal.com/shop>

Draft for Public Comment

STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Committee OB-007—Risk Management

DRAFT

Australian/New Zealand Standard

Business continuity—Managing disruption-related risk

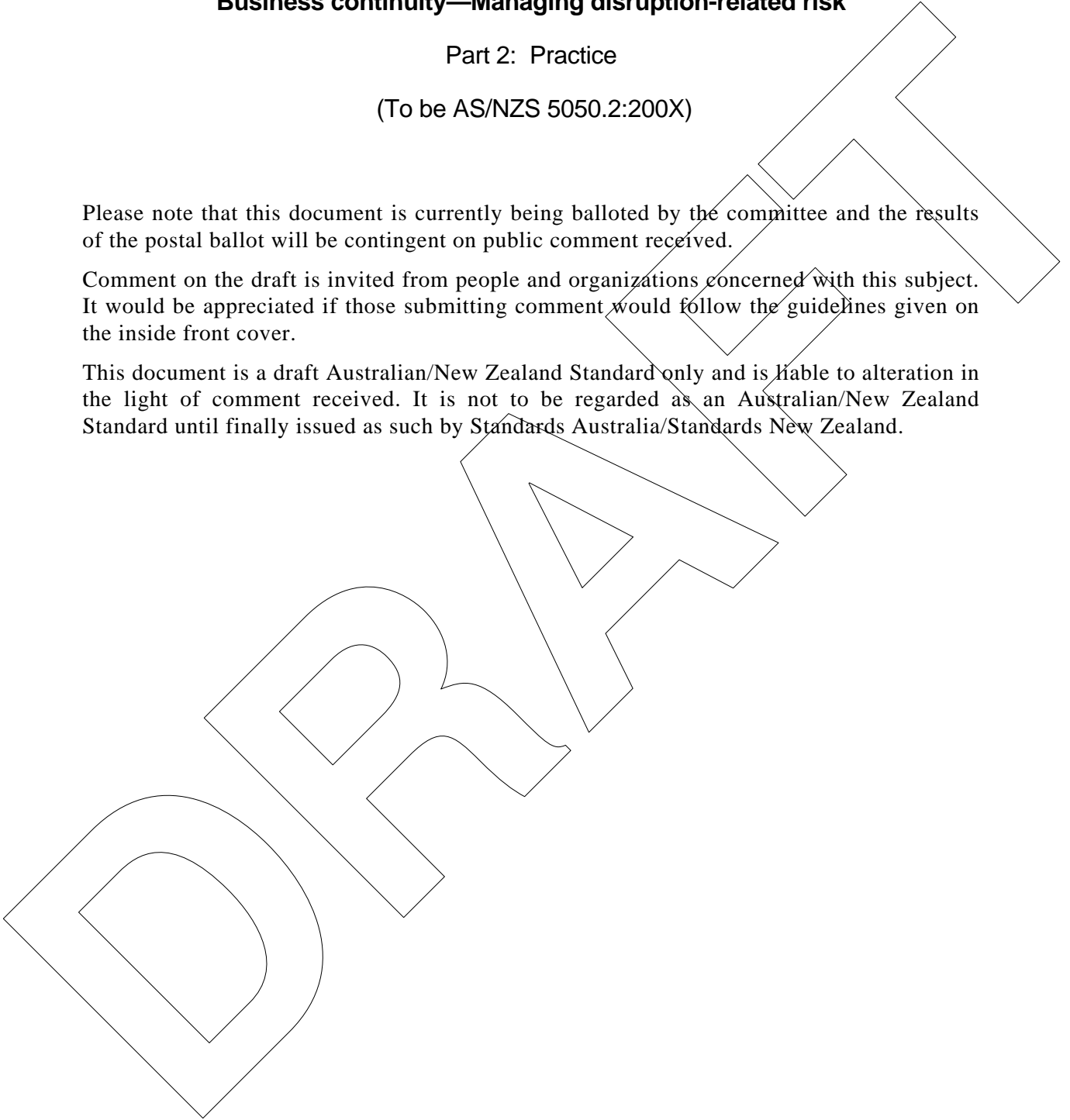
Part 2: Practice

(To be AS/NZS 5050.2:200X)

Please note that this document is currently being balloted by the committee and the results of the postal ballot will be contingent on public comment received.

Comment on the draft is invited from people and organizations concerned with this subject. It would be appreciated if those submitting comment would follow the guidelines given on the inside front cover.

This document is a draft Australian/New Zealand Standard only and is liable to alteration in the light of comment received. It is not to be regarded as an Australian/New Zealand Standard until finally issued as such by Standards Australia/Standards New Zealand.



PREFACE

This Standard was prepared by Standards Australia/Standards New Zealand Committee OB-007, Risk Management.

Business Continuity Management (BCM) is a form of risk management activity to assess and where appropriate treat the risk that disruption may prevent or hinder organizations achieving their strategic, operational and project objectives. It therefore contributes to making organizations more resilient and consequently may provide strategic and tactical advantage.

Effective BCM requires a deep understanding of the organization's objectives and operating environment (including its dependencies) in order to identify the sources of this type of risk and the mechanisms through which the organization's objectives can be disrupted. Such understanding also allows the organization to make advance preparations in order to minimize the effects of what otherwise would be disruptive events, particularly those of a scale which (without BCM techniques) are outside the capacity of the routine management approaches to deal with effectively. The preparations are aimed at—

- (a) early stabilization;
- (b) continuation or early resumption of operations, particularly those which are most critical to the organization's objectives;
- (c) minimization of and prompt recovery from any adverse effects; and
- (d) realizing any opportunities created by the event.

Additionally, the insight provided by the BCM process, will frequently point to cost effective measures which would reduce either the magnitude or likelihood of events which can cause disruption. In many cases it will be a more cost effective and successful means of ensuring business continuity to implement such treatments than it will be to rely on contingent planning. This emphasises the importance of BCM activity being integrated into the overall risk management activity, and therefore into the organization's governance and management systems.

For this reason, BCM methodology follows general risk management methodology as described in ISO 31000:2009 and is strongly focused on the organization's objectives.

This Standard is presented in three parts, as follows:

AS/NZS

- 5050 Business continuity—Managing disruption related risk
- 5050.1 Part 1: Specification
- 5050.2 Part 2: Practice (This Standard)
- 5050.3 Part 3: Assurance

Each of the above parts is suited to any form of organization or community entity in the public, private and not-for profit sectors. For convenience the term 'organization' is used throughout the Standard to denote any or all of these types of entity.

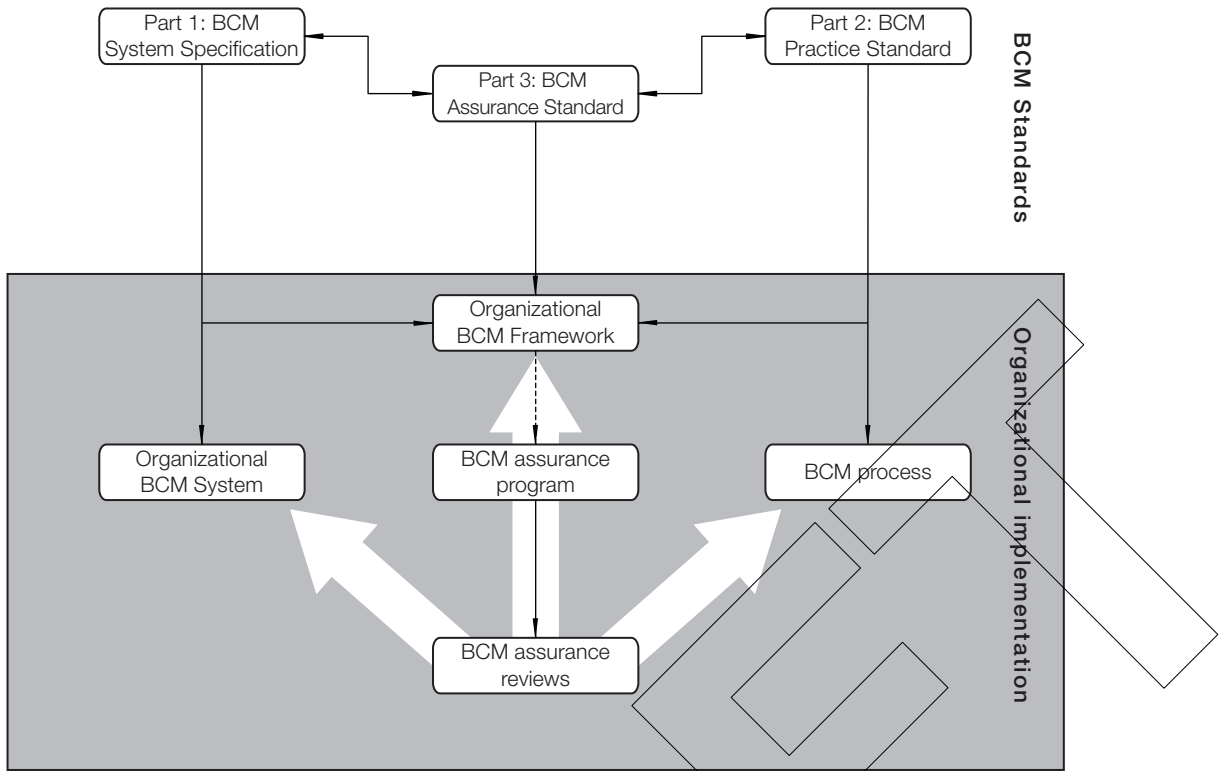


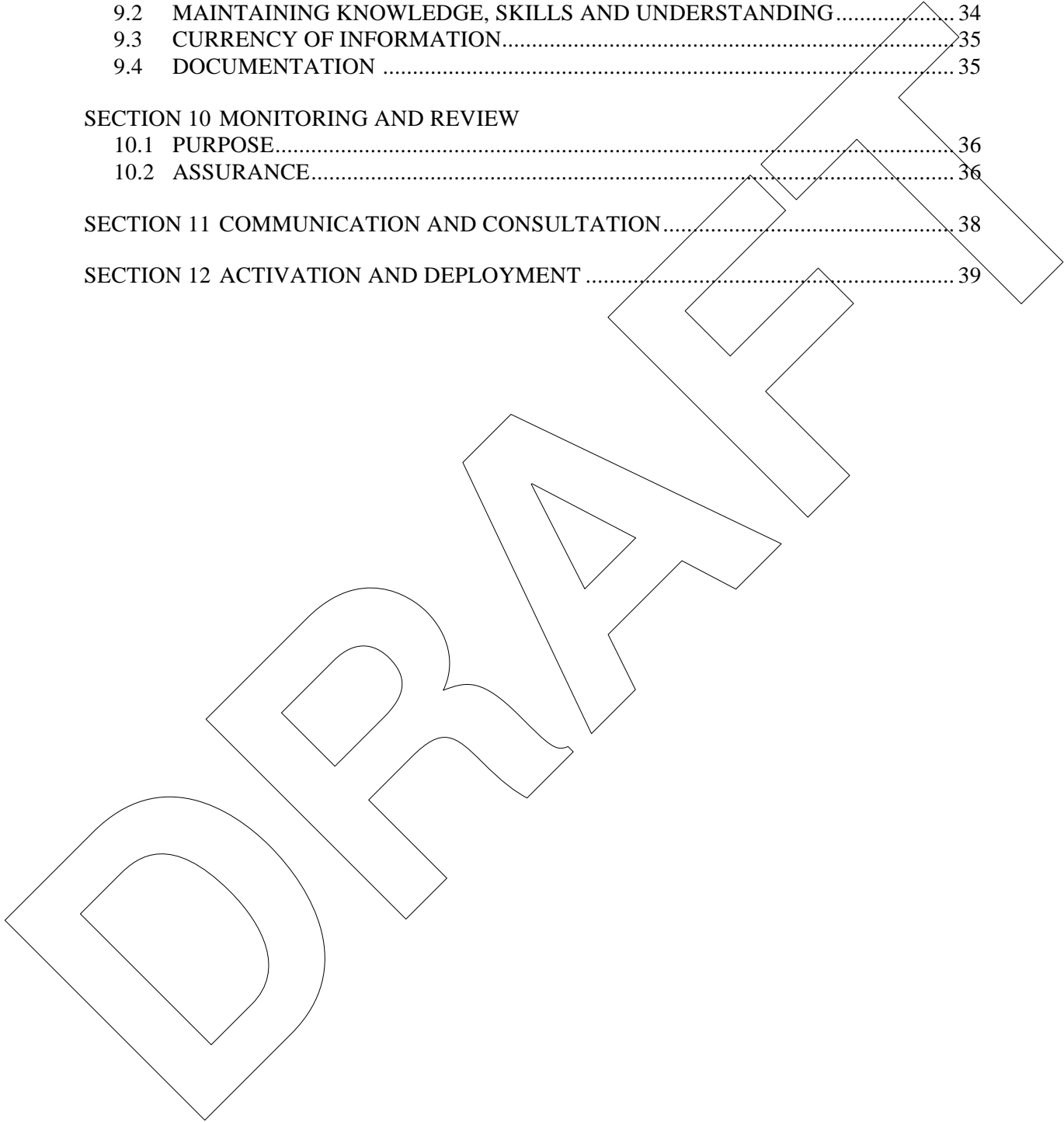
FIGURE P1 BCM STANDARDS' RELATIONSHIPS AND THEIR IMPLEMENTATION

DRAFT

CONTENTS

	<i>Page</i>
SECTION 1 SCOPE AND GENERAL	
1.1 SCOPE	6
1.2 DEFINITIONS.....	6
1.3 REFERENCED DOCUMENTS.....	9
1.4 BACKGROUND	9
1.5 DEFINING BUSINESS CONTINUITY MANAGEMENT	10
1.6 BCM IN THE MANAGEMENT OF RISK.....	10
1.7 THE BENEFITS OF INVESTING IN BCM.....	11
SECTION 2 OVERVIEW OF BUSINESS CONTINUITY MANAGEMENT	
2.1 GENERAL.....	12
2.2 PRINCIPLES OF BCM	12
SECTION 3 THE FRAMEWORK FOR BCM	
3.1 GENERAL.....	14
3.2 COMMENCEMENT AND COMMITMENT	14
3.3 DESIGN OF THE BCM FRAMEWORK	16
3.4 DOCUMENTATION OUTPUTS	17
3.5 IMPLEMENTING BCM.....	17
3.6 MONITORING AND REVIEW OF THE BCM FRAMEWORK	18
3.7 CONTINUAL IMPROVEMENT OF THE BCM FRAMEWORK.....	18
SECTION 4 THE PROCESS FOR BCM	19
SECTION 5 ESTABLISHING UNDERSTANDING	
5.1 GENERAL.....	21
5.2 ESTABLISHING THE CONTEXT	21
SECTION 6 RISK ASSESSMENT	
6.1 RISK ASSESSMENT PROCESS OVERVIEW	23
6.2 RISK IDENTIFICATION.....	23
6.3 RISK ANALYSIS	23
6.4 CONDUCTING A BUSINESS IMPACT ANALYSIS	23
6.5 DOCUMENTATION OUTPUTS	26
6.6 EVALUATION.....	26
SECTION 7 DEVELOPING CAPABILITIES	
7.1 GENERAL.....	27
7.2 DEVELOPING AND ANALYSING DISRUPTION MANAGEMENT STRATEGIES	27
7.3 DEVELOPING STABILIZATION STRATEGIES.....	27
7.4 DEVELOPING CONTINUITY STRATEGIES	28
7.5 DEVELOPING BUSINESS RECOVERY STRATEGIES.....	29
7.6 DEVELOPING INCIDENT MANAGEMENT STRATEGIES.....	30
7.7 ESTABLISHING RESOURCES AND INTERDEPENDENCIES.....	30
7.8 DOCUMENTATION OUTPUTS	30
7.9 DEVELOPING EVENT COMMUNICATION AND CONSULTATION	30

	<i>Page</i>
SECTION 8 CREATING PLAN DOCUMENTATION	
8.1 DOCUMENTING ISSUES.....	32
8.2 DEVELOPING THE FRAMEWORK AND FORMAT OF PLANS.....	32
SECTION 9 ESTABLISHING MAINTENANCE PROCESSES	
9.1 GENERAL.....	34
9.2 MAINTAINING KNOWLEDGE, SKILLS AND UNDERSTANDING.....	34
9.3 CURRENCY OF INFORMATION.....	35
9.4 DOCUMENTATION	35
SECTION 10 MONITORING AND REVIEW	
10.1 PURPOSE.....	36
10.2 ASSURANCE.....	36
SECTION 11 COMMUNICATION AND CONSULTATION.....	38
SECTION 12 ACTIVATION AND DEPLOYMENT	39



STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Australian/New Zealand Standard
Business continuity—Managing disruption-related risk**Part 2: Practice**

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE

This Standard describes the establishment of a BCM framework, the program that implements this framework, and the practices of business continuity management (BCM) that support it. Business Continuity Management (BCM) is an approach that helps organizations achieve their strategic, operational and project objectives by enabling them to better manage disruption-related risk. BCM can provide a powerful means to gain strategic and tactical advantage and enhance organizational resilience.

BCM is an approach aimed at reducing the occurrence, severity and adverse effects of disruptive events (including capture of any opportunities which may be created by such events). It is particularly focused on types of disruption which exceed the capacity of the routine management system to resolve.

Business continuity management is an iterative process. Steps must be carried out in a logical order and the results of earlier activities must be reviewed in light of what is learned in subsequent steps. Its elements include prevention, and preparations for stabilization, continuation (or early resumption) of critical functions, recovery and return to routine sustainable management control.

The Standard is designed for use by organizations of any size and complexity in public, private and not-for-profit sectors.

1.2 DEFINITIONS

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

1.2.1 Activation

The process whereby all or a portion of the stabilization, business continuity or recovery plans have been put into action.

1.2.2 Alternate site

An alternate operating location to be used when particular primary facilities are inaccessible. Another location, computer centre or work area designated for recovery with necessary infrastructure and resources.

NOTE: Also referred to as 'alternative work area', 'recovery site', or 'alternate location' ('alt loc').

1.2.3 Backlog

The amount of work that accumulates when a system or process is unavailable.

NOTES:

- 1 This work needs to be processed once the system or process is available and may take a considerable length of time to clear.
- 2 In extreme circumstances, the backlog may become so large it may not be cleared or resolved.

1.2.4 Business continuity plan

A collection of procedures and information that is developed, compiled and maintained in readiness for use should an event occur which would otherwise disrupt the organization or its through chain.

NOTE: The expression business continuity planning is often used to refer to those activities associated with preparing documentation to assist in the continuing availability of property, people, information and processes.

1.2.5 Business continuity program (BCM)

A BC program is the planned implementation of the BCM process into the whole, or selected areas of the organization according to agreed criteria.

1.2.6 Business impact analysis (BIA)

A management level analysis, which assesses the risks associated with disruption, including a consideration of the required resources, interdependencies and the nature, impact and likelihood of capability loss over time.

NOTES:

- 1 The BIA characterizes and measures the effects of capability loss, including those of escalating losses over time and effects on interdependencies, in order to provide senior management with reliable data upon which to base decisions on risk treatment and planning for stabilization, continuity and recovery
- 2 Also referred to as business impact assessment.

1.2.7 Business interruption

Any event, whether anticipated or unanticipated which disrupts the organization's normal course of routine operations.

1.2.8 Consequence

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.

1.2.9 Crisis

A situation where organizations shift from routine to non-routine operation, requiring management to divert a proportion of their attention, time, energy and resources away from normal operations to managing this event.

1.2.10 Critical business functions

Vital functions without which an organization will either not survive or will lose the capability to effectively achieve its critical objectives.

NOTES:

- 1 A critical business function can comprise a single process or several processes contributing to a final definable output.
- 2 A critical business function may involve a single structural unit of the organization, or may involve activities across several structural units.
- 3 A single structural unit may have responsibility for one or more critical business functions.

1.2.11 Critical objectives

Those objectives, as determined by the organization, which must continue to be achieved.

1.2.12 Disaster recovery planning

Activities associated with the continuing availability and restoration of infrastructure.

1.2.13 Disruption-related risk

The chance of experiencing consequences resulting from an event either within or exterior to the organization that prevent or impair routine operations to such a scale as to be beyond the capacity of the routine management approaches to resolve.

1.2.14 Emergency

An event, actual or imminent, which endangers or threatens to endanger people or achievement of the organization's goals (including its compliance obligations), and which is significant and requires a timely and coordinated response.

1.2.15 Event

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', 'near hit', or 'close call'.

1.2.16 Likelihood

Chance of something happening.

NOTE: 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).

1.2.17 Maximum acceptable outage (MAO),

The maximum period of time that an organization can tolerate the disruption of a critical business function, before its ability to achieve its objectives is adversely affected.

NOTE: Also known as maximum tolerable outage (MTO), maximum downtime (MD), maximum tolerable period downtime (MTPD).

1.2.18 Recovery

Following the commencement of an event, recovery is the implementation of strategies and procedures in order to return the organization to a sustainable level of capability and operation.

NOTE: The organization may be recovered to its pre-disruption status, to a different type or level of capability, or changed strategic direction.

1.2.19 Recovery point objective (RPO)

The capability at a pre-disruption point in time to which systems and data must be recovered after an outage (e.g. to end of previous day's processing).

1.2.20 Recovery time objective (RTO)

The period of time required to fully re-establish adequate resources to recover a critical activity, process, function, or other capability, to a required minimum operational level.

NOTE: The time required to recover capability to achieve the RPO may be additional to the RTO.

1.2.21 Risk

Effect of uncertainty on objectives.

NOTES:

- 1 An effect is a deviation from the expected - 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, consequences, or a combination of these and how they can affect the achievement of objectives.
- 4 Risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances, and the associated likelihood of occurrence.

1.2.22 Stakeholder

Any 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.

1.2.23 Through chain

The end to end value chain encompassing the supply, process and distribution chains, including information, knowledge and financial flows.

1.2.24 Uncertainty

State, even partial, of deficiency of information related to or understanding of or knowledge of an event, its consequence, or likelihood.

1.3 REFERENCED DOCUMENTS

The following documents have been referenced in this Standard.

AS/NZS

5050 Business continuity-Managing disruption related risk

5050.3 Assurance

HB

436 Risk Management Guidelines Companion to AS/NZS 4360:2004

ISO

31000 Risk Management—Principles and guidelines on implementation

1.4 BACKGROUND

The current volatile environment has seen the emergence of increasing risks associated with personal safety, food, water and energy security, through chain integrity, infrastructure availability, human resource capability, cashflow availability, criminality, and governance breaches. It is highly likely that these issues, and others still to emerge, will continue to dominate societal concerns for the foreseeable future. In response to this, many public, private and not-for-profit entities are placing more emphasis and focus their need for the improved management of risk. This has been accompanied by increasing expectations of customers, regulators and the public for the uninterrupted availability of services and products.

This environment now places a growing importance on the need, in all sectors, for effective BCM. Not just established for technological systems, but also covering all critical strategic and operational activities.

Present and future volatility will present both significant threats and opportunities that organizations will need to manage through improved business continuity.

1.5 DEFINING BUSINESS CONTINUITY MANAGEMENT

This Standard adopts the following definition for BCM:

‘Business continuity management is a proactive strategic and operational approach that aims to ensure the continuing capability of people, processes, infrastructure, resources and information that provide for the achievement of critical objectives, when faced with potential disruption.

1.6 BCM IN THE MANAGEMENT OF RISK

BCM as described within this Standard is a logical and iterative process for managing risks to the continuity of those operations necessary for achieving the objectives of the organization. To be effective BCM must be integrated into the strategy and operations of the organization and be undertaken as a long term activity within the organization’s risk management arrangements.

Effective management of disruption-related risks requires—

- (a) an understanding of the organization’s objectives, its internal and external environment; risk criteria and stakeholders;
- (b) identification of the organization’s critical objectives, resources, processes and interdependencies;
- (c) an assessment of the risks;
- (d) development and implementation of strategies that will reduce the likelihood and scale of disruptive events and to reduce adverse impacts of such events while taking advantage of resulting opportunities;
- (e) flexibility in BCM strategies and actions to meet unanticipated events; and
- (f) consideration of, and alignment of the BCM strategies with the organization’s culture.

Although, traditionally, BCM has tended to place greatest emphasis on disruption-related risks with high consequence, it has been recognised that frequent lower consequence events can also seriously degrade the organization’s capacity.

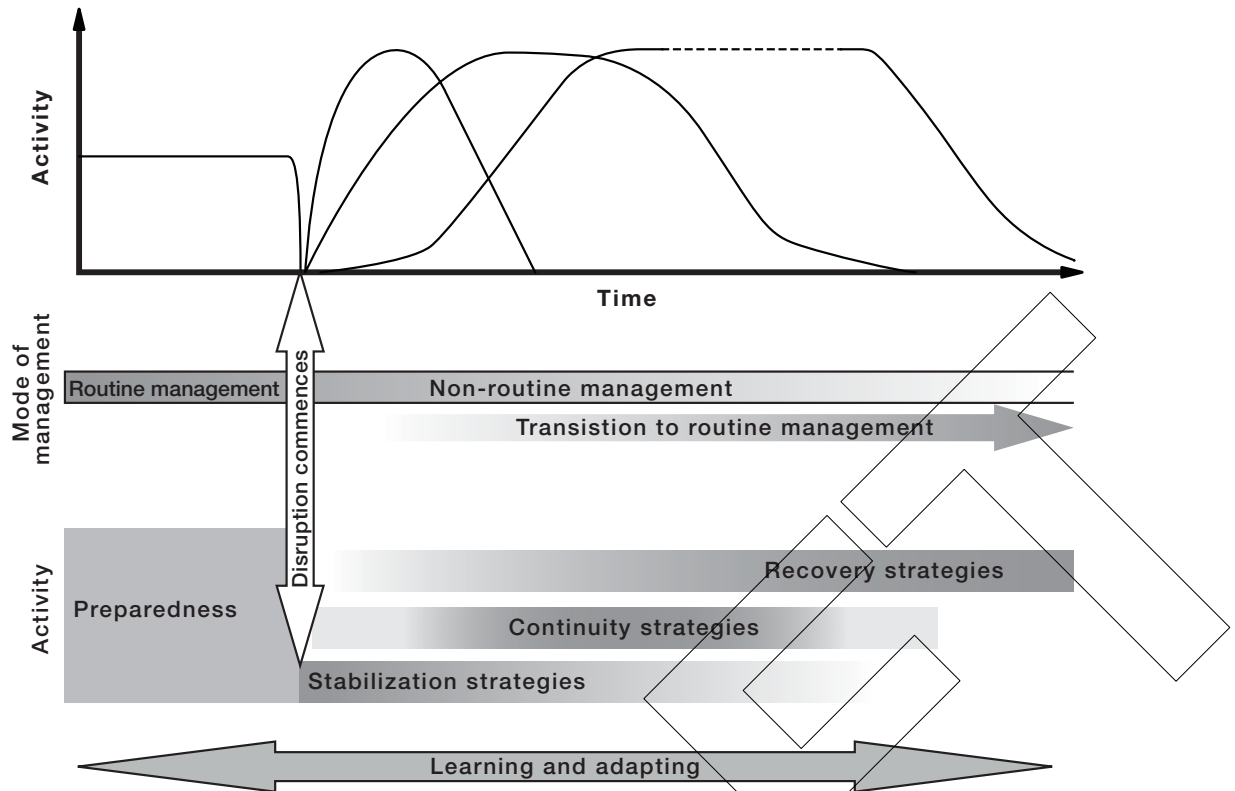


FIGURE 1 KEY AREAS OF ACTIVITY OCCURRING WITHIN BCM

It is also important to remember that disruption-related risks are only a portion of the risks that an organization needs to manage.

1.7 THE BENEFITS OF INVESTING IN BCM

BCM, when implemented appropriately, will provide a robust framework for addressing disruption-related risk in a cost effective and timely manner. The time, effort and resources devoted to BCM should be regarded as a prudent investment by an organization that will return a range of benefits, including—

- (a) improved preparedness to respond to and manage a wide range of unanticipated events or other occurrences;
- (b) a mechanism for protecting shareholder interests and promoting stakeholder confidence;
- (c) a means of helping to ensure continuing operational capability in the face of an increasingly volatile environment;
- (d) improved capability to ensure ongoing legislative compliance;
- (e) a strong means of sustaining improved corporate governance;
- (f) a means of reducing revenue leakage;
- (g) enhanced capability to protect the customer base and market share; and
- (h) improved protection of reputation and brand value.

SECTION 2 OVERVIEW OF BUSINESS CONTINUITY MANAGEMENT

2.1 GENERAL

There are three important areas of consideration in BCM (see Figure 2), namely the principles of BCM, the framework for BCM and the process for BCM.

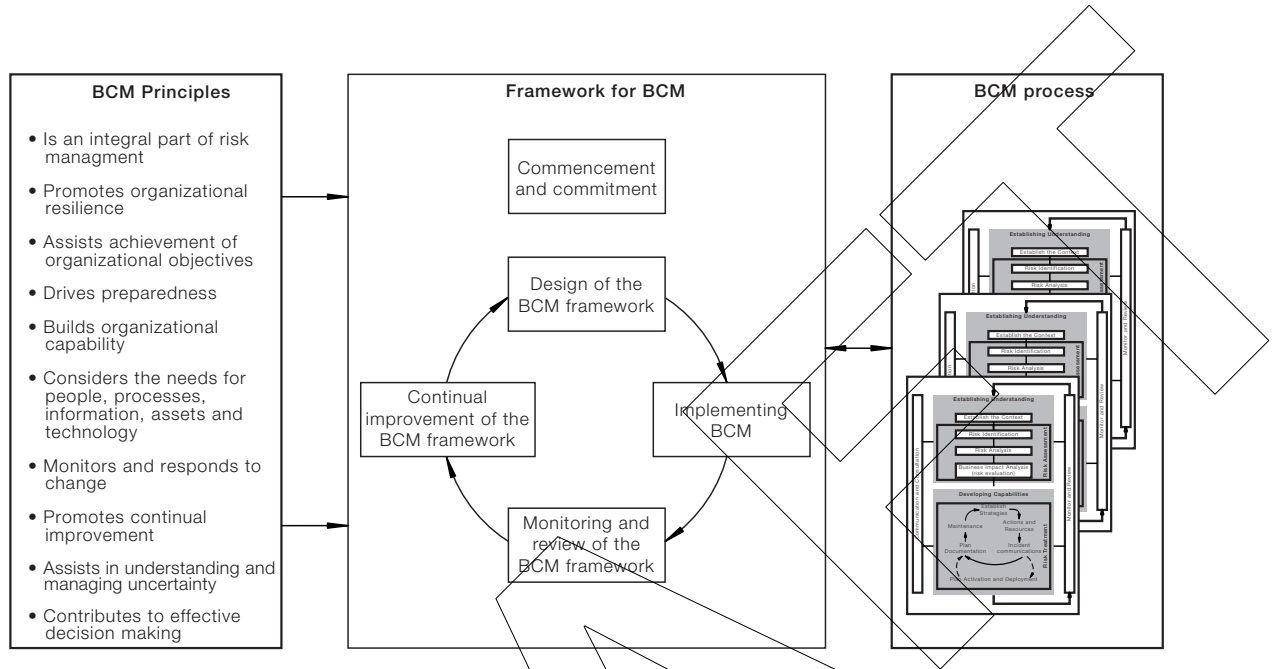


FIGURE 2 THE INTERRELATIONSHIPS OF THE BCM PRINCIPLES, FRAMEWORK AND PROCESSES

2.2 PRINCIPLES OF BCM

To be effective BCM should pay attention to the following principles:

- (a) *Is an integral part of risk management*—BCM is part of a well founded approach to organizational risk management that considers a wide range of strategic and operational risks to continuity of critical business objectives.
- (b) *Promotes organizational resilience*—BCM is an important contributor to the organization’s adaptive capacity in a complex and changing environment.
- (c) *Assists achievement of organizational objectives*—BCM assists the organization to continue to achieve its critical organizational objectives by—
 - (i) reducing the likelihood and scale of disruptive events;
 - (ii) reducing the impacts of such events through implementing its stabilization strategies;
 - (iii) providing the capability to continue to achieve those objectives through implementing its continuity strategies; and
 - (iv) returning the organization to a sustainable level of operation through its recovery strategies.

- (d) *Drives preparedness*—BCM drives the organization’s preparedness for managing future potentially disruptive events, by treating risk including by establishing capability to manage impacts of future potential events.
- (e) *Builds organizational capability*—BCM builds the organization’s capability to affect the likelihood of events occurring and to respond to, manage and recover from the events’ impacts, where such capability includes people, facilities, information, processes, technology and other equipment.
- (f) *Considers the needs for people, processes, information, assets and technology*—BCM seeks to understand the organization’s needs for people, processes, information, assets and technology that will contribute to the achievement of its critical business objectives and that are required to assist in the efficient and effective conduct of BCM.
- (g) *Is iterative and responsive to change*—BCM is an iterative process that is continually monitoring and reviewing the external and internal contexts for change and driving the organizations BCM framework and process to respond to that change. At each step of the BCM process new understanding will emerge that will challenge earlier assumptions, again driving an iterative monitoring, review and improvement throughout the process.
- (h) *Promotes continual improvement*—The iterative nature of BCM, in responding to change, drives continual improvement of the BCM framework and the BCM process, thus contributing to organizational preparedness and resilience.
- (i) *Assists in understanding and managing uncertainty*—BCM is focused on creating an improved understanding of uncertainty in the external and internal contexts and in how the organization could respond to and manage that uncertainty.
- (j) *Contributes to effective decision making*—BCM provides an analytical framework which assists decision makers in making informed choices on the management of disruption risk and events. It provides the means for making judgments on the cost-benefits of various strategic and operational options and the most effective way of implementing those options.

SECTION 3 THE FRAMEWORK FOR BCM

3.1 GENERAL

It is the BCM framework that provides the foundations, structures and capabilities to enable effective BCM to be carried out and to be embedded within the organization. The BCM framework assists in the establishment of an effective BCM process for managing disruption risks and events. The BCM framework (see Figure 3) needs to be established such that it reflects the organization’s internal and external contexts and to meet the organization’s and key stakeholders requirements for BCM. As such the framework may have to be customised by the organization to meet specific requirements and changes in context. The framework enables effective management of disruption-related risks through the BCM process.

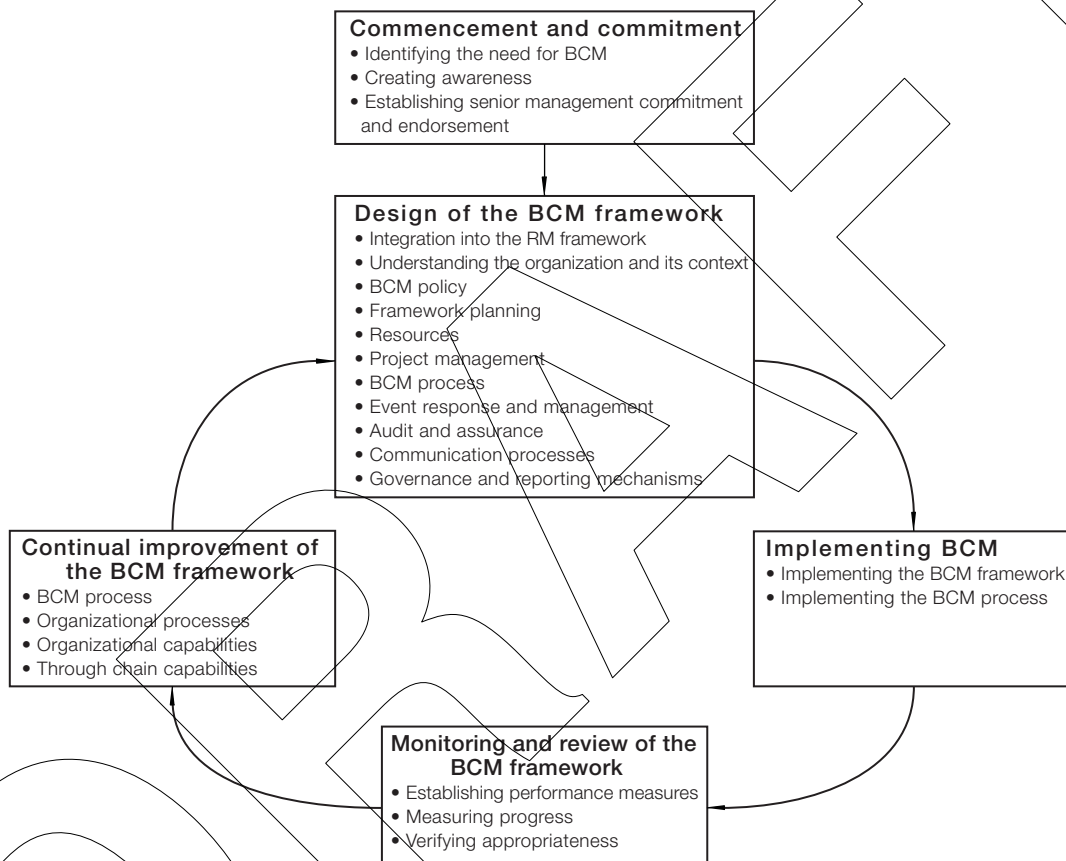


FIGURE 3 THE BCM FRAMEWORK

3.2 COMMENCEMENT AND COMMITMENT

Initial activities are concerned with commencement of the development of the BCM framework, or enhancement of existing risk management frameworks and gaining the commitment of managers and staff to BCM. This includes the following:

- (a) *Identifying the need for BCM*—The need for an organization to introduce BCM or expand its existing approach could be driven by a number of factors, including—
 - (i) identification, analysis and evaluation of disruption-related risks;
 - (ii) regulatory requirements;

- (iii) contractual requirements;
 - (iv) competitive advantage;
 - (v) common industry practice;
 - (vi) improved governance;
 - (vii) increasing volatile environment;
 - (viii) stakeholder expectations; and
 - (ix) previous experiences of disruptions or near misses.
- (b) *Creating awareness*—Initial activities should focus on enhancing or creating an awareness of BCM and the organization's need for it, with key decision makers being involved as early in the process as practicable. The early adoption of a senior management champion for BCM can greatly assist in developing and driving through a BCM program. This can include—
- (i) what the BCM framework and process entails;
 - (ii) the reasons why BCM is required for the organization or by key stakeholders;
 - (iii) how BCM will be, or is being, approached by the organization;
 - (iv) the benefits to the organization, both tangible and intangible, in undertaking BCM;
 - (v) the resource implications of undertaking BCM; and
 - (vi) the responsibilities for managing BCM within the organization.

As the scope of BCM activities is expanded and it is implemented through different areas of the organization, the awareness activities may have to be repeated with different managers and other key staff.

The extent to which commitment and engagement activities are undertaken should be based on cost-benefit analysis. Activities that could be considered include—

- (A) creating or establishing an improved awareness and understanding of the need for BCM and the benefits that are likely to accrue from it;
 - (B) providing benchmarking information on the sectoral status of BCM; and
 - (C) providing case study examples of organizations that have failed to respond to or that have shown resilience to significant disruption events.
- (c) *Establishing senior management commitment and endorsement*—It will be important to gain (or reinforce) the commitment of management at all levels within the organization, in order to develop and sustain BCM, to address—
- (i) continuing demands on management time and attention;
 - (ii) any distractions from other core activities;
 - (iii) competition for resources that may occur;
 - (iv) requirements to make decisions on issues based on information arising from BCM activities;
 - (v) cultural change that may be driven by BCM or that need to occur for BCM to be fully effective;
 - (vi) emerging information that challenges organizational orthodoxy, priorities and individual management beliefs; and

- (vii) any requirements to make material changes to be made to some routine parts of the organization's operations.

These activities should engender the effective engagement of stakeholders in the BCM program and should be reinforced on an ongoing basis.

The use of a well prepared business case can also serve to enhance commitment to BCM as well as provide an effective means of gaining endorsement from senior management.

3.3 DESIGN OF THE BCM FRAMEWORK

The principal activities that need to be considered in designing the BCM framework include the following:

- (a) Integration of BCM activities into the organization's general risk management activities.
- (b) Understanding the organization and its context is a critical first step since the organization and its context are the critical drivers of the requirements for BCM, this will significantly affect the design of the BCM framework.
- (c) BCM policy position should be developed that reflects the aims and objectives agreed to in the approved scope and provides guidance on the design of the BCM process, its conduct and the responsibilities and expectations of key stakeholders. The policy should consider—
 - (i) the organization's rationale for undertaking BCM;
 - (ii) accountabilities and responsibilities for BCM;
 - (iii) the structures and processes used for BCM;
 - (iv) resources required for BCM;
 - (v) how governance will be addressed and reported; and
 - (vi) the manner and metrics by which the performance of BCM will be assessed.
- (d) *Scope and framework planning*—the finalization of a scope will need to be undertaken in consultation with managers responsible for critical business functions and senior management. The scope will determine the subsequent design and planning for the BCM framework.
- (e) *Resources*—infrastructure and resourcing should be established to implement and maintain the BCM framework. This should also include requirements for developing required resource capabilities such as procurement, re-engineering, training and development.
- (f) *Project management*—effective project management principles should be adopted to provide the means of implementing the framework and managing the program of BCM activities
- (g) *BCM process*—a BCM process should be designed that meets the agreed scope and policy requirements.
- (h) *Event response and management*—a structure and processes for activating and coordinating the response to an event and the implementation of other strategies should be established.
- (i) *Audit and assurance*—processes for the provision of audit and assurance of the BCM framework, BCM process and its outputs should be established.

- (j) *Communication processes*—a consultation and communications strategy should be created to assist in the development and implementation of the BCM framework and process. This should include a specific recognition of mechanisms for enhancing engagement of key stakeholders.
- (k) *Governance and reporting mechanisms*—consideration should be given to the necessary governance requirements for the BCM framework, including accountabilities, responsibilities, authorities, compliance requirements and reporting requirements.

3.4 DOCUMENTATION OUTPUTS

During this part of the BCM program a range of documentation (paper and electronic) may be produced, including—

- (a) detailed scope;
- (b) business case;
- (c) policy;
- (d) communications and engagement strategy;
- (e) BCM framework and program resourcing plan;
- (f) detailed or summary statements describing the context;
- (g) training needs analysis;
- (h) role competency statements; and
- (i) completed checklists.

3.5 IMPLEMENTING BCM

Effective implementation of BCM requires—

- (a) Implementing the BCM framework, for example by—
 - (i) determining how the plan (developed in Clause 3.3(c)) will be implemented and project managed;
 - (ii) project managing to agreed objectives, schedules, resource availability and to the delivery of agreed outputs;
 - (iii) aligning the implementation of the framework with other organizational frameworks, programs, processes;
 - (iv) ensuring that all compliance requirements are met;
 - (v) conducting awareness and training sessions; and
 - (vi) continuing to communicate and consult with stakeholders to ensure the ongoing relevance of the BCM framework.
- (b) Implementing the BCM process—The BCM process is implemented by ensuring that the activities outlined in Section 5 are undertaken in a considered and logical manner, supported by an appropriate level of resourcing.

3.6 MONITORING AND REVIEW OF THE BCM FRAMEWORK

BCM should be conducted in a manner that ensures it continues to perform effectively and continues to assist in the achievement of critical objectives. The organization should therefore—

- (a) establish measures against which the performance of the BCM framework can be assessed;
- (b) measure the conduct of the BCM framework to ensure that required progress is occurring; and
- (c) on a regular basis verifying that the framework is still appropriate for any changes in context or capability that have occurred.

3.7 CONTINUAL IMPROVEMENT OF THE BCM FRAMEWORK

The organization should consider the requirements for continual improvement of the BCM framework and its constituent parts. Decisions on implementing improvements should be based on the outputs from the monitoring and review (undertaken in Clause 3.5). Improvement options may include enhancing—

- (a) the BCM process;
- (b) other organizational processes;
- (c) organizational capabilities (people, assets, information, technology, culture); and
- (d) through chain capabilities.

SECTION 4 THE PROCESS FOR BCM

The essential components of the BCM process comprise—

- (a) developing an understanding of the concept of risk, and awareness and understanding of the organization's objectives and the environment it operates within as the source of disruption-related risk;
- (b) developing capabilities through—
 - (i) identifying and implementing strategies for the treatment of disruption-related risk;
 - (ii) defining actions and developing resource requirements and their interdependencies;
 - (iii) identifying internal and external communications for managing an event;
 - (iv) preparing plans and documenting measures to be put in place to address stabilization, continuity and recovery strategies and actions; and
 - (v) maintaining these capabilities, including the plans and resources;
- (c) developing communication and consultation, regarding the day-to-day conduct of the business continuity process (as opposed to communications concerned with managing an actual disruption or activation of plans); and
- (d) monitoring and reviewing the conduct and performance of the BCM process and introducing improvements or other activities as required to meet changing contexts and/or organizational requirements.

BCM is an iterative process whereby the outcomes of each stage are used to challenge and review the assumptions and outcomes of previous stages, through the monitoring and review process (see Figure 4).

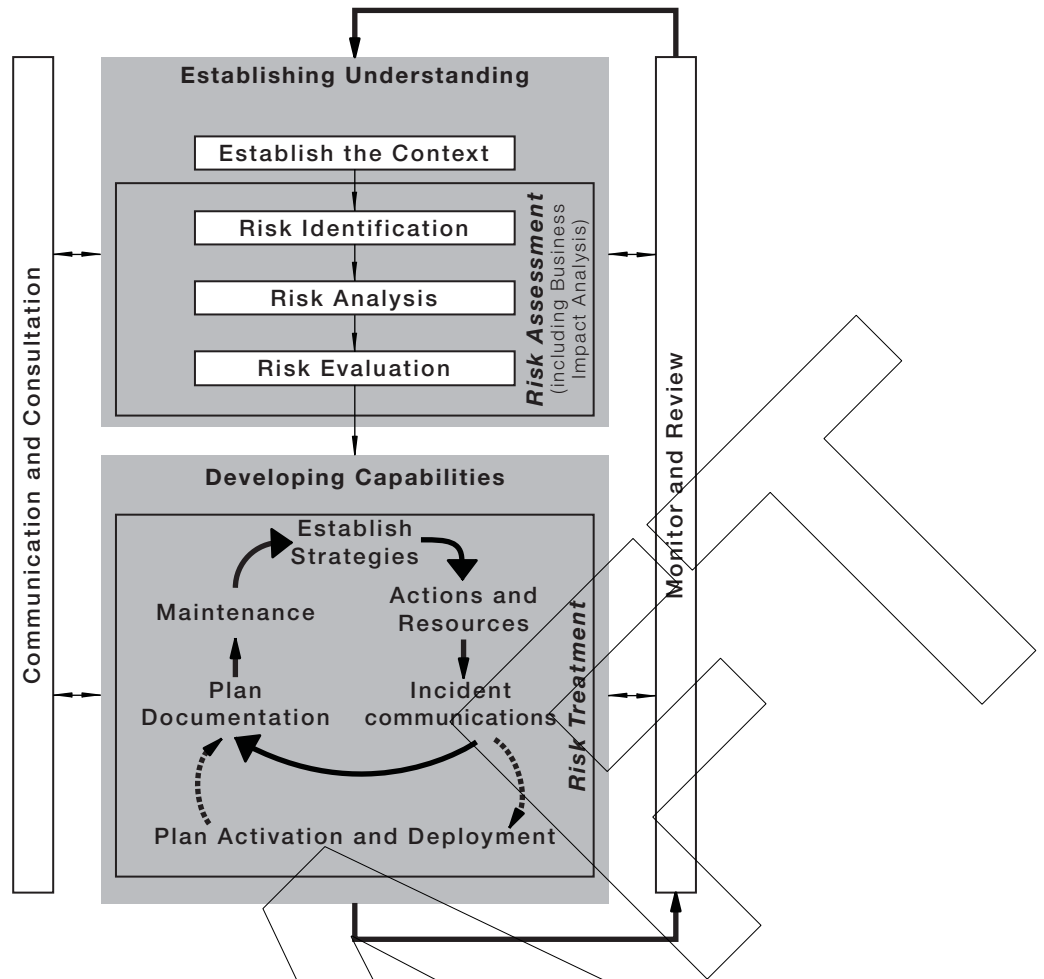


FIGURE 4 THE BCM PROCESS

BCM goes well beyond implementing a simple process and writing a business continuity plan (BCP). The plans need to be flexible and decision makers need to appreciate the uncertainty and complexity. BCM should reflect the organization's culture and comprise a comprehensive set of activities that are appropriately integrated into the organizational learning and improvement.

SECTION 5 ESTABLISHING UNDERSTANDING

5.1 GENERAL

It is essential that the organization establishes an understanding of why it should implement BCM, what will drive the requirements for the BCM process, and what the BCM process will need to manage.

BCM considers those risks associated with disruption of the organization's ability to manage using routine practices and capacity and prevent achievement of critical objectives. Many of the events with the capacity to cause this level of disruption are of a non-routine nature and are often outside of the common experience of management. They are typically characterised by high levels of uncertainty, complexity and ambiguity, and are usually, but not always, characterised by high consequence with low likelihood.

This will require that an understanding of risk and how the organization's objectives and the environment that it operates within, gives rise to disruption-related risk. This will involve—

- (a) establishing the context;
- (b) conducting assessment of disruption-related risks; and
- (c) identifying necessary treatments

5.2 ESTABLISHING THE CONTEXT

Establishing the context involves gathering information from a variety of sources in order to be clear as to the organization's objectives, gaining a thorough understanding of how the organization operates, what its priorities are, how it interacts with its external and internal environments, who are its stakeholders, what are its risk criteria and what current and emerging issues (both operational and strategic) need to be considered. The context will provide guidance in developing aims and objectives for the BCM program, creating the scope and documenting the subsequent business case.

The following four aspects of the context need to be considered:

- (a) *The external context*—consideration should be given to examining, for example, issues in the—
 - (i) physical environment (e.g. natural hazards and events);
 - (ii) built environment (e.g. land use, urban planning, critical infrastructure, neighbouring facilities);
 - (iii) socio-political environment (legislation, community issues, demography, regional security); and
 - (iv) industrial and market environment (e.g. market status, emerging markets, competitor activity, supply chains).
- (b) *The internal context*—consideration should be given to examination of the organization's objectives, articulating as clearly as possible all of the organization's objectives drawing on, for example—
 - (i) statutory functions; statements of intent; vision and mission statements; strategic plans including those relating to specific parts of the organization;
 - (ii) public statements regarding the organization's goals and statements of intent to other stakeholders;

- (iii) determination of (mission) critical objectives;
 - (iv) initial identification of critical business functions, critical processes, critical personnel, critical assets, critical elements or aspects of the through chain and critical information flows; and
 - (v) identification of current or emerging issues that may result in, increase the vulnerability to, or contribute to the likelihood or impact of potentially significant disruption.
- (c) *The stakeholders*—identification of persons and organizations that can affect, be affected by, or perceive themselves to be affected by the organization's ongoing ability to conduct its business.
- (d) *The organization's risk criteria*—determining the terms of reference against which disruption-related risks will be evaluated.

In each of the foregoing, particular consideration should be given to—

- (A) the relevance of issues identified in the internal and external context to the needs, development and implementation of BCM;
- (B) how these issues will be reflected in specific aims and objectives for BCM;
- (C) the identification of any imperatives that will dictate the scope and structure of BCM;
- (D) how BCM needs to be undertaken (i.e. which critical areas of the organization will be included, which will not); and
- (E) expected deliverables and outcomes from the proposed BCM program.

SECTION 6 RISK ASSESSMENT

6.1 RISK ASSESSMENT PROCESS OVERVIEW

A robust process for assessing risk must be followed (for example ISO 31000). Risk should be assessed on the basis of consequences and their likelihood using predetermined evaluation criteria that allow for the prioritization of any necessary treatments. It is important that consequence is considered broadly, for example—

- (a) financial;
- (b) reputational;
- (c) stakeholder;
- (d) social and community;
- (e) people;
- (f) operational;
- (g) strategic; and
- (h) legal, statutory and regulatory.

6.2 RISK IDENTIFICATION

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. Documents, such as existing risk registers should be considered and may facilitate the identification of additional disruption related risks.

6.3 RISK ANALYSIS

The identified risks should be analysed, considering factors that affect consequences and their likelihoods, including the effectiveness of existing controls. The way in which consequence and likelihood are used to provide ratings of risk may vary under different contexts and should be consistent with the developed risk criteria. Risks that exceed the risk criteria and which are unlikely to be controlled by routine management capability should be selected for more a detailed examination in the Business Impact Analysis.

6.4 CONDUCTING A BUSINESS IMPACT ANALYSIS

The business impact analysis (BIA) ensures a more detailed insight into the extent, time frames and mechanisms of disruptive consequences associated with the priority disruption-related risks assessed in the previous steps and thus also assists in evaluating those risks. The key steps in conducting the BIA are summarized in Figure 5.

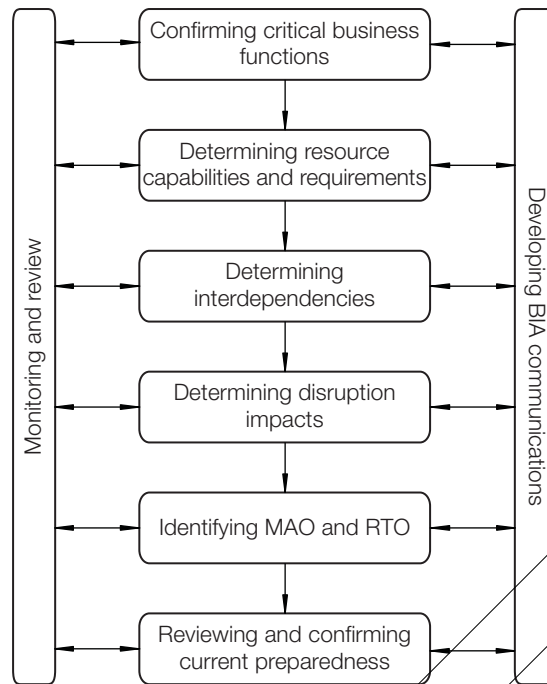


FIGURE 5 THE BUSINESS IMPACT ASSESSMENT

Step 1—Developing BIA communications and consultation

The BIA is a major information gathering exercise and requires building trust and the cooperation of a range of individuals within (and perhaps external to) the organization. Methods for communicating with and consulting with BCM stakeholders will need to be developed. Communications and consultation plans should cover the intent of the BIA, what types of information will be required, how this information will be collected and how it will be used.

Step 2—Confirming critical business functions

The nominated critical business functions (identified in both establishing the context and the risk assessment) are confirmed as appropriate and such designation should be approved by the appropriate senior manager. This may result in some previously identified functions being removed and additional critical business functions being added in to those being considered in the BIA. The critical business functions will be subsequently prioritized based on their maximum acceptable outage (MAO) as described in Step 6.

Step 3—Determining resource capabilities and requirements

Current resource requirements should be identified for each critical business function (business as usual). The level of required resourcing, following a disruptive event, should be determined for sustaining capability to deliver the minimum acceptable level of functionality. Types of resources that should be considered include the following:

- (a) People (staff, management, volunteers).
- (b) Information and data, including vital records, SOPs.
- (c) Accommodation, facilities, plant and equipment.
- (d) IT and telecommunications systems.
- (e) Critical infrastructure.
- (f) Transportation.
- (g) Consumable supplies.

- (h) Finances.
- (i) General assets, supplies and other consumables.
- (j) Third party suppliers, contractors and other external supporting resources.

Where applicable the capabilities, type, number, size for each essential resource should be determined. For some types of resources it may be beneficial to determine how resources requirements may change over time until routine capability is re-established. Any interdependencies that may affect access to, availability of, and/or the performance of resources should also be identified.

Step 4—Determining interdependencies between capabilities, resources and stakeholders

Existing interdependencies, as well as those that emerge during or following the disruption event, should be identified and mapped. These interdependencies are likely to involve the organization’s stakeholders and resources, as well as other business processes.

Step 5—Determining the disruption impacts

The assessment of impact on each critical business function should be considered over a range of time periods that a disruption could occur. Time periods should be selected that are relevant to the context and the critical business function.

Step 6—Identifying the maximum acceptable outage and recovery time objectives

The maximum acceptable outage (MAO) should be determined for each critical business function. This is generally the disruption time after which the organization can no longer tolerate the loss or degradation of capability of the critical business function (see Figure 6).

The organization should also estimate the recovery time objective (RTO). This is the time period by which it is expected that resource requirements for each critical business function will be recovered, or could be reasonably restored or recovered. The level of resource recovery should be such that the critical business function is capable of operating at minimum acceptable operational level. These resource requirements are generally based on the need to recover IT capability, but may also encompass other resource capabilities such as other infrastructure, people, important processes or other support activities.

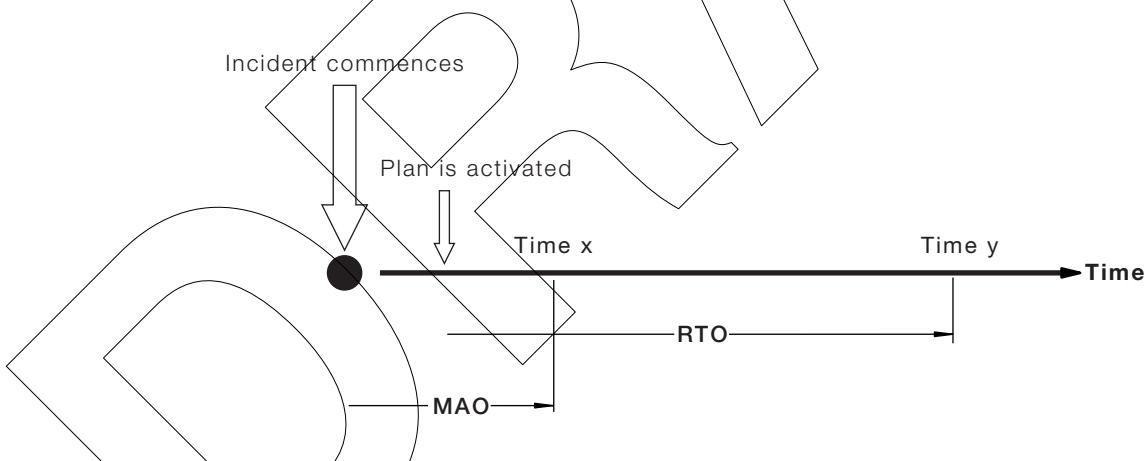


FIGURE 6 THE RELATIONSHIPS BETWEEN A MAXIMUM ACCEPTABLE OUTAGE (MAO) AND A RECOVERY TIME OBJECTIVE (RTO)

Where there is a significant time gap between the MAO time and the RTO, strategies will need to be considered which will enable the critical business function to continue to an acceptable minimum standard until recovery is achieved. Strategies that reduce the RTO should be considered in conjunction with, or as alternatives to extending the MAO.

It is important to note that the MAO period commences as soon as the disruption occurs, however the RTO commences only when plans are activated and recovery actions commence. The effective gap between the MAO and RTO could therefore be significantly longer than the apparent gap in documented times.

For some critical business functions it may also be necessary to identify a recovery point objective (RPO). This represents the point in time, prior to the disruption, to which data should be recovered. The RTO assists in identify the scope of any data processing backlogs that must be managed.

Step 7—Identifying alternate workarounds

Where it is possible that the capability of a critical business function will be insufficient to achieve the critical business objectives, various options for alternative workarounds may need to be identified. It is possible that some workarounds already exist or are readily apparent. Such workarounds such be identified and documented at this step and could include the following:

- (a) Alternate processes, for example using a manual process in place of an automated process.
- (b) Delimited functions, for example where ‘unnecessary’ processes, or parts thereof, are halted, allowing only the most critical elements of the processes to operate.
- (c) Outsourcing the critical business functions or dependant processes.
- (d) Bypass and re-routing.
- (e) Hibernating functions or processes until such time that required capability can be established, recovered, and/or maintained.

Step 8— Reviewing and confirming current preparedness

The current level of preparedness (including existing strategies plans and resources), should be reviewed in light of the identified potential impacts. In particular the capability for addressing the MAO time and achieving the RTO should be examined and the extent of any perceived gaps in capability should be confirmed.

6.5 DOCUMENTATION OUTPUTS

The documentation outputs from the risk assessment should include for each critical business function—

- (a) a register of risks, reviewed and updated following completion of the BIA
- (b) identified MAO times, RTOs and RPOs;
- (c) a resource register and interdependency maps;
- (d) a list of identified alternate workarounds;
- (e) a list of stakeholders and their interdependencies; and
- (f) a map of interdependencies amongst critical business functions.

6.6 EVALUATION

Evaluation of the risks assists in making decision on the need to treat the risks based on the outcomes of the initial risk assessment and subsequent business impact analysis. The risk criteria (established during the context development) should be considered in determining the organization’s and other key stakeholders tolerance of the risk. This should also take into account any legal, regulatory or other requirements.

The evaluation may lead to the decision to not treat certain risks.

SECTION 7 DEVELOPING CAPABILITIES

7.1 GENERAL

Treatment of disruption-related risks may require treatments to reduce the likelihood or scale of disruptive events or to reduce the disruptive consequences of such events. The latter may include adding to the organization's capabilities and capacity to deal with non-routine situations. Treatments may need to be developed for both pre and post commencement of an event. The selection of appropriate risk treatments should be based on the evaluation of a range of options that should consider—

- (a) reducing any negative consequences and/or their likelihood;
- (b) enhancing any positive consequences and/or their likelihood;
- (c) sharing the risk with other parties; and
- (d) avoiding the risk by discontinuing the activities that create it.

Selection of the mix of treatments should be made following the conduct of a cost benefit analysis.

7.2 DEVELOPING AND ANALYSING DISRUPTION MANAGEMENT STRATEGIES

Strategies for managing disruptions and their impacts should consider how the chances of future events occurring can be reduced and, how consequences and their likelihood can be enhanced, reduced, shared or avoided. These strategies should be aimed at enhancing the capabilities of people, assets, infrastructure, processes and the through chain.

Developing disruption management strategies requires that approaches for stabilization, continuity and recovery are considered. Strategy options (i.e. possible risk treatments) should be subjected to a cost benefit analysis, and should also consider—

- (a) extent of compliance with regulations, government policy, industry standards, and organizational policies of each alternative;
- (b) availability and suitability of options;
- (c) alignment with other controls, treatments and capabilities;
- (d) total cost of developing, implementing and maintaining each option (including, financial, time, performance, costs);
- (e) prospect of generating new risks or creating further loss or harm;
- (f) capability of the organization to implement each of the alternative options;
- (g) extent to which each option assists in achieving the agreed BCM objectives; and
- (h) other tangible and intangible benefits.

7.3 DEVELOPING STABILIZATION STRATEGIES

The overall aim of the stabilization strategies is to minimise the level of organizational impact and reduce any losses following the commencement of an incident. Issues that should be considered include—

- (a) reviewing existing strategies, plans and procedures for completeness, relevance and currency;
- (b) matching existing strategies to the identified priority risks and potential disruptions to ascertain any gaps in coverage;

- (c) improving existing strategies and developing new strategies to address any shortfalls;
- (d) identifying any inter-linkages between the stabilization, continuity and recovery strategies and proposed activities;
- (e) ensuring that responsibilities are in place for understanding and managing compliance with regulatory requirements; and
- (f) ensuring that activation triggers are identified for individual strategies.

Strategies that could be considered include—

- (i) emergency response involving the immediate preservation of life and property;
- (ii) containment, such as preventing the spread of further harm;
- (iii) suppression, such as reducing the impacts that are causing harm;
- (iv) isolation, such as removing critical resources from harm; and
- (v) loss control, such as preventing leakage of funds.

7.4 DEVELOPING CONTINUITY STRATEGIES

7.4.1 Overall aim

The overall aim of the continuity strategies is to ensure the ongoing delivery of an accepted minimum level of organizational capability and performance, following an event or other occurrence. This will require that decisions are made in consideration of—

- (a) the circumstances under which continuity plans may be activated (the activation triggers);
- (b) required approaches to manage the consequences and/ or their likelihood of disruption-related risks identified earlier in the process;
- (c) the effectiveness and need to improve (or reduce or remove) existing control measures and capabilities;
- (d) organizational priorities;
- (e) the selection of the most appropriate option identified through the BIA to achieve the key objectives and priorities;
- (f) the delegation of new authority to individuals; and
- (g) criteria for salvaging, sourcing and transporting of critical resources from the disrupted site or from alternate locations.

7.4.2 Capabilities

Strategies will need to be developed to address maintaining, developing or introducing the following capabilities:

- (a) People capabilities.
- (b) Facility and infrastructure capabilities (including data, communication and information capabilities).
- (c) Through chain capabilities.
- (d) Other critical stakeholder capabilities.
- (e) Critical business function and process capabilities.

Such strategies could include—

- (i) continuity of operations, such continuing critical business objectives;

- (ii) continuity of strategy; ensuring that maintained activities support key strategic objectives;
- (iii) consequence management, such as reducing collateral harm or exploiting emerging opportunities;
- (iv) hibernation, such as reducing or ceasing non-critical activities;
- (v) salvage, such as removing and repairing damaged assets; and
- (vi) leakage control, reducing items of non-essential expenditure.

7.5 DEVELOPING BUSINESS RECOVERY STRATEGIES

The overall aim for business recovery strategies is to return the organization to a long term operationally acceptable and sustainable capability. This may involve recovering the business to its pre-disruption capability, developing a new, improved or expanded capability, or a completely different business model altogether. There will be some limits as to the level of detail that can be developed for business recovery strategies as they will usually be very dependant upon the nature of the disruption experienced.

However, in general terms, the organization should document its decisions and steps in strategic preparedness, such as—

- (a) identifying key recovery and restoration objectives;
- (b) determining requirements and protocols for undertaking environmental scanning prior to and during the recovery operations (in order to inform decision making regarding recovery priorities, directions and activities);
- (c) approaches for the management of processing backlogs generated in the aftermath of the disruption event;
- (d) identification of members of the prospective recovery team(s);
- (e) developing a project management methodology and coordination framework for managing the recovery process;
- (f) requirements for insurance claims management;
- (g) document and data recovery and restoration protocols;
- (h) development of testing protocols to ensure re-establishment of capability to required sustainable levels; and
- (i) establishing a learning capability, that can, in particular, be subsequently used to investigate the causes and effects of actual disruptions (and near misses) that may occur, including—
 - (i) protocols for conducting process, systems and engineering failure analysis, and
 - (ii) investigations of control breaches (e.g. OHS, security, fraud) .

Recovery strategies may include—

- (A) functional restoration, such as bringing the operation of critical business functions to sustainable levels;
- (B) capability recovery, such as re-establishing optimum resource levels;
- (C) infrastructure restoration, such as rebuilding damaged facilities, networks or plant;
- (D) operational redevelopment, such as re-designing work areas or re-engineering processes;
- (E) withdrawal or divestment, such as moving out of selected markets, locations, or industries; and

- (F) performance improvement, such as investing in enhanced process quality.

7.6 DEVELOPING INCIDENT MANAGEMENT STRATEGIES

The organization should develop strategic options for implementing the plans, activating capabilities, deploying resources and for the overall coordination of stabilization, continuity and recovery activities. These issues are dealt with more fully in Section 12.

7.7 ESTABLISHING RESOURCES AND INTERDEPENDENCIES

Once the stabilization, continuity and recovery strategies have been established, it will be necessary to ensure that there will be appropriate and adequate resource capabilities to support them.

Information on current and projected resource requirements that has been collected across multiple critical business functions should be collated and mapped in order to determine—

- (a) any redundancies in resources available, for example for salvage and re-deployment elsewhere;
- (b) any conflicting demands or synergies with required resources;
- (c) types, volumes and duration of use requirements for each resource required;
- (d) current location for each of the identified resources, and contact details for individuals in control of them; and
- (e) identification of any interdependencies (internal and external) in the sourcing, application or disposal of these resources.

A gap analysis should be conducted to compare these resource requirements against current capabilities in order to identify new or expanded resource capability that need to be further developed.

7.8 DOCUMENTATION OUTPUTS

Consideration should be given to the need for the following documentation:

- (a) Supplier and customer contracts.
- (b) Service level agreements.
- (c) Warranties.
- (d) Insurance schedules and certificates of currency.
- (e) Resource temporary transfer and return agreements.
- (f) Resource lists and allocation plans.
- (g) Directories of emergency/alternate suppliers
- (h) Asset registers.

7.9 DEVELOPING EVENT COMMUNICATION AND CONSULTATION

As part of BCM communication and consultation, consideration should be given to the communication and consultation required should a disruption occur and to developing plans for such an eventuality.

The development of strategies for these event communication and consultation' should consider—

- (a) purpose;

- (b) scope, including—
- (i) identity of the stakeholders and audience;
 - (ii) types, breadth and depth of information to be provided or sought;
 - (iii) means and media that will be used to communicate the information;
 - (iv) frequency of communication releases and consultation activities;
 - (v) areas of the organization that will be involved in crafting; approving and distributing communications and conducting consultation; and
 - (vi) legal, social, language, confidentiality, technical constraints that need to be considered.
- (c) communication and consultation planning issues, including—
- (i) development of 'templates' or prescribed forms of communication and consultation;
 - (ii) agreed processes for crafting; reviewing and approving communications and consultations;
 - (iii) processes for receiving; assessing and distributing in-bound communications;
 - (iv) guidelines for developing message content;
 - (v) specific identification of mode or channels for each specific type of communication and consultation;
 - (vi) identification of assumptions made in developing communications and consultation including intended audiences;
 - (vii) assessment of organizational capabilities for the required scope of communication and consultation;
 - (viii) requirements for ensuring accessibility to the communications and consultation; and
 - (ix) delegations of authority to approve content and release of information.

SECTION 8 CREATING PLAN DOCUMENTATION

8.1 DOCUMENTING ISSUES

Both electronic and hardcopy documentation of plans are acceptable, so long as access to these plans will not be adversely affected by a disruption. Documented plans need to be written in such a way that they can be read, easily understood and exercised by those that will be expected to activate and implement them. Attention therefore needs to be paid to the following criteria in documenting the various plans:

- (a) Simplicity and clarity of the concepts and instructions.
- (b) Use of language and terminology appropriate to the audience and organization.
- (c) Flexibility to adapt to changing circumstances.
- (d) Sufficiently comprehensive information to ensure that the plans are workable.
- (e) Necessary and sufficient brevity of the information provided, such as the need for succinctness for rapid access.
- (f) Achievable in the circumstances within which they will be deployed.
- (g) Accessible when required.
- (h) Confidentiality is maintained where necessary.
- (i) Different plans complement, not conflict with each other.

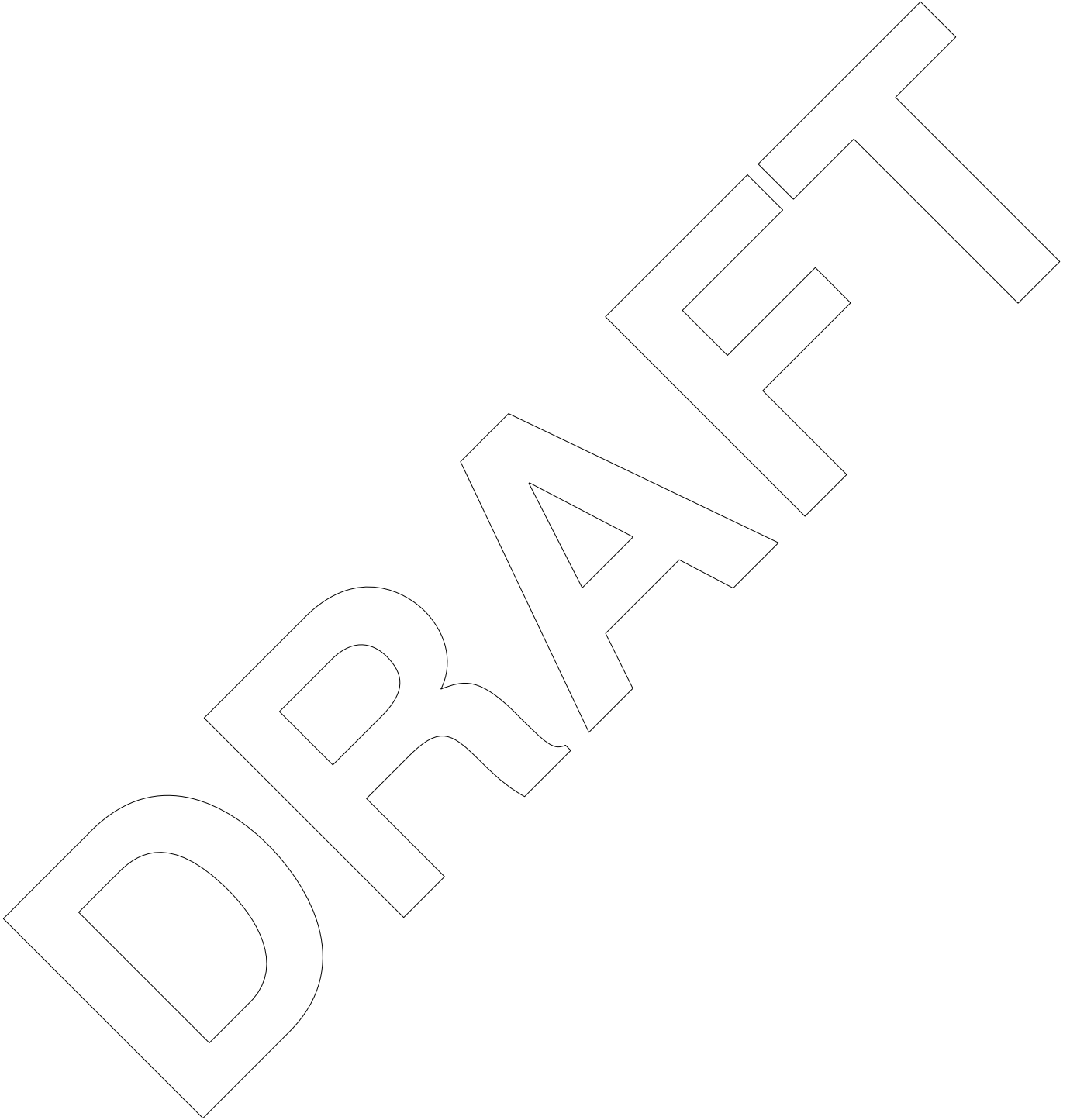
8.2 DEVELOPING THE FRAMEWORK AND FORMAT OF PLANS

The framework and format of plans needs to be designed to fit the context and needs of the organization. For example small to medium organizations, may require only one or two simple plans (for example an evacuation plan and a business continuity plan). However, a larger or more complex organization may require separate plans catering for different scenarios, sites, critical business functions, critical assets, special dates or time periods. Consideration be given to needs for documenting overarching coordination plans where multiple plans may need to be activated following an event (for example: 'critical incident management plan, crisis management plan, incident response plan).

The content of individual plans will usually be determined by the organization (to meet its specific needs including any contractual or regulatory obligations); however, there are some common elements that should be incorporated in all plans—

- (a) version and date of the document should be clearly identified;
- (b) authors, reviewers and approvers should be identified and sign off;
- (c) plan objectives and scope should be clearly described;
- (d) criteria should be documented for activation and stand-down of the plans;
- (e) specific roles accountabilities and responsibilities should be identified for all named positions;
- (f) adequate procedural descriptions should be provided for all required processes and workarounds;
- (g) all essential resource requirements, their locations and any special access or allocation requirements should be documented;

- (h) communication and consultation plans should be identified for key internal and external stakeholders;
- (i) contact lists should be provided for key employees, contractors, consultants, suppliers, customers and other priority stakeholders; and
- (j) accommodation and other facility arrangements should be detailed, including maps or plans where necessary and should also be provided for alternate sites.



SECTION 9 ESTABLISHING MAINTENANCE PROCESSES

9.1 GENERAL

Organizational capabilities and plans developed through the BCM program must operate as intended when called upon. Apart from Monitoring and Review activities to check ongoing relevance and currency (refer to Section 10) some elements of the BCM arrangements (for example, the maintenance of necessary knowledge and skills) will require planned maintenance actions in order to be effective when called upon. The scope and frequency of necessary maintenance activities for each element should be determined at the time the element is designed and those activities should be included in the design. Maintenance activities will address two main areas—

- (a) knowledge, skills and understanding; and
- (b) currency of information;

9.2 MAINTAINING KNOWLEDGE, SKILLS AND UNDERSTANDING

The effectiveness of some aspects of the BCM arrangements will require that particular individuals or those occupying specific positions have particular knowledge, skills and understandings. The principal methods to achieve this are routine training with associated testing, and exercising of knowledge and skills by applying them to relevant scenarios and simulations. The latter also contributes to ongoing monitoring and review of the adequacy of the BCM arrangements.

Exercises can be designed and conducted so that they provide—

- (a) participants with an improved awareness of the organizational context and priorities;
- (b) participants with an improved understanding of the content and use of plans;
- (c) participants with improved confidence in responding to incidents;
- (d) participants with an opportunity to improve their capabilities;
- (e) an assessment of the utility and applicability of the developed strategies;
- (f) an evaluation of the adequacy of developed capabilities and resource allocations;
- (g) an identification of previously undocumented requirements and practices employed in managing an incident or disruption;
- (h) an opportunity to identify any other inadequacies in the written plans and their implementation;
- (i) an opportunity to identify areas or functions that could be hibernated or limited in their use of resources;
- (j) assurance that plans are capable of being implemented when required;
- (k) confidence to stakeholders regarding the organization preparedness; and
- (l) a means of fulfilling regulatory, contractual or organizational governance requirements.

There are a number of different types of exercise that can be undertaken. The decision as to the suitability of the type of exercise will depend upon the context for BCM, the objectives for the exercise, budget and participant availability and the tolerance of the organization to operational disruption caused by holding the exercise.

The principal types of exercise are—

- (i) desktop walkthrough, which aims to provide an enhanced understanding of the components and structures of the plans through a review and guided discussion using the plans;
- (ii) desktop review which combines a review of the plans in light of one or more hypothetical disruption scenarios;
- (iii) discussion exercise where questions are posed based on hypothetical disruption scenarios;
- (iv) full scale (deployment) exercise, which involves a 'live' activation of plans based on a hypothetical scenario(s);
- (v) recovery tests, which involves either closing down or removing access to key elements of systems or infrastructure and the recovery of alternate capability;
- (vi) notification and communications call out involves the activation of key personnel and tests the ability to reach contacts identified within the plan; and
- (v) other approaches such as interviews, seminars and workshops that allow individuals to provide information on their responsibilities and capabilities and to share experiences and concerns with responding to incidents.

9.3 CURRENCY OF INFORMATION

It is to be expected that some information forming part of plans or other elements of the BCM arrangements will require routine updating. Arrangements for such updating must be put in place and wherever possible, be automated whereby new or revised information created for normal operational purposes (for example, the names of individuals in the organization chart) is automatically copied into BCM plans which relate to that information.

9.4 DOCUMENTATION

BCM maintenance activities (for example, the de-brief of exercises) should be documented as part of the BCM arrangements with the scope and form of documentation meeting governance, regulatory and contractual obligations as well as the specific needs of the BCM arrangements. Such documentation will also provide input to routine monitoring and review and continuous improvement.

SECTION 10 MONITORING AND REVIEW

10.1 PURPOSE

In addition to maintenance activities, all aspects of the BCM arrangements and their planning and development require routine monitoring and periodic review to provide assurance of ongoing relevance, readiness and effectiveness.

This includes monitoring of information relied upon or generated by the BIA and review of continuing appropriateness of assumptions on which the BCM arrangements are based. This should provide confirmation and currency of—

- (a) critical organizational objectives and accepted or stipulated performance levels;
- (b) routine operating resource capabilities;
- (c) locations of and interdependencies between stakeholders, critical business functions, processes, resources and the extended through chain;
- (d) vulnerabilities in the extended through chain;
- (e) disruption related impacts upon the identified critical business functions in both financial and operational terms;
- (f) essential performance metrics such as the MAO, RTO and RPO;
- (g) roles and responsibilities within critical business function;
- (h) contact details of key stakeholders;
- (i) options for alternate workarounds; and
- (j) the capabilities of existing plans to manage the issues and requirements identified through the BIA.

10.2 ASSURANCE

Assurance activities within the monitor and review arrangements should provide verification and validation of the BCM program and the content and application of the plans developed through the process. Assurance activities should examine both the status of capabilities and their performance in action.

The mix and methods of assurance activities should be efficient (both in cost and time) and may include—

- (a) exercises (refer to Clause 9.2);
- (b) self assessment of specific elements or components of individual plans (component testing);
- (c) a technical assessment of plan capabilities (such as a systems recovery test);
- (d) a compliance audit against a documented framework, policy, standard procedure, contractual or legislative requirement; and
- (e) performance audit that examines the efficiencies and effectiveness of a BCM program;

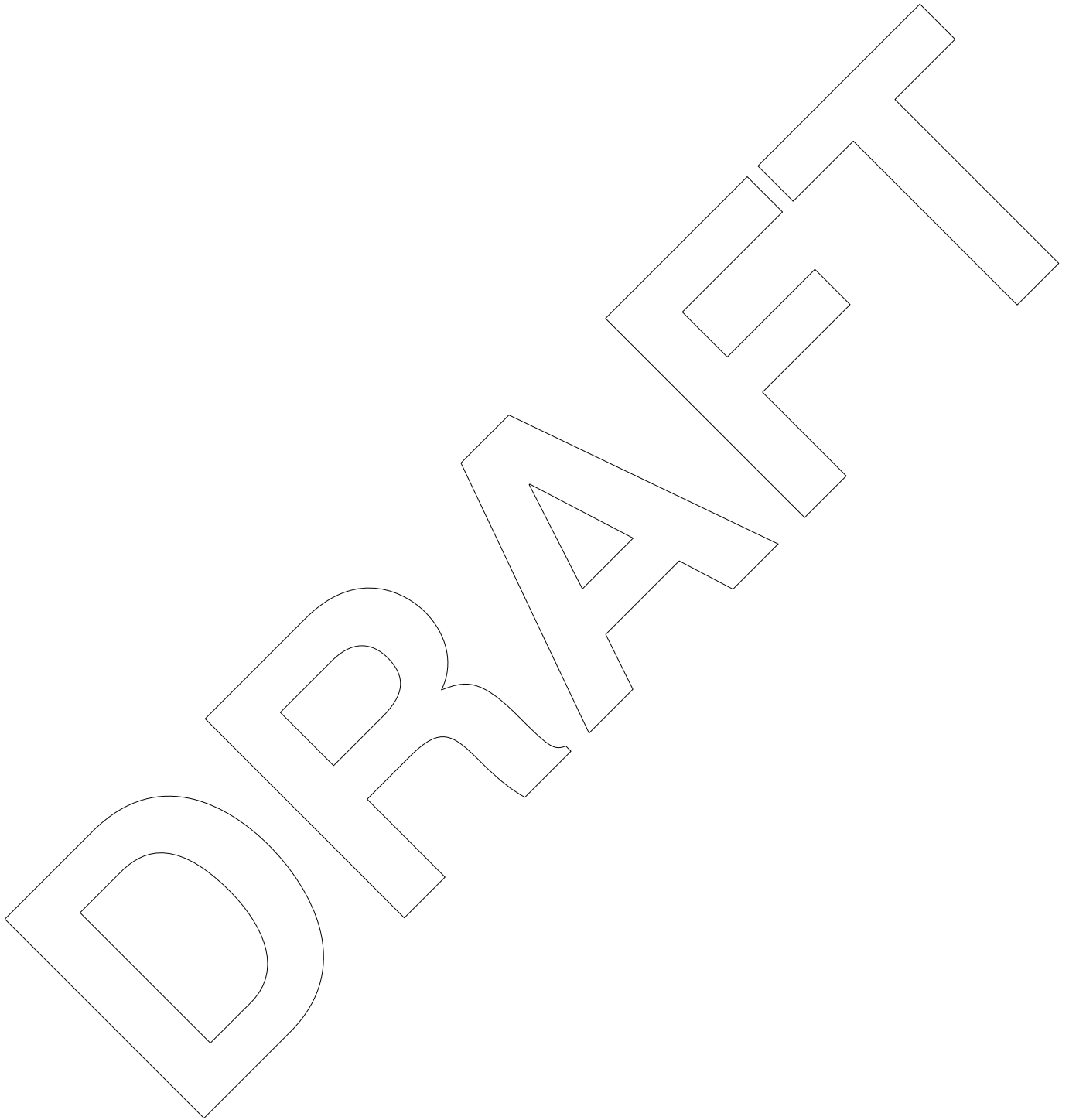
Assurance methods may include—

- (i) semi-structured staff checks and structured self assessments;
- (ii) management review;
- (iii) internal audit review; and

(iv) external audit review.

Useful guidance on the design of assurance arrangements can be found in HB 436:2004 and AS/NZS 5050.3.

Whatever combination of assurance activities are selected, they should, ultimately, provide a comprehensive examination across all key aspects of the BCM program, the documented plan(s) and the required capabilities.



SECTION 11 COMMUNICATION AND CONSULTATION

Developing effective communication and consultation with both internal and external stakeholders at each stage of the BCM process is a necessary component of the BCM process. It should therefore be planned from the outset, with the plan identifying stakeholders, timelines, resource requirements and specific purposes.

Communication and consultation activities inform stakeholders about the existence and purpose of the BCM arrangements and the expected effects on stakeholders, and provides a means of soliciting information required to undertake the planning.

Specific communication and consultation activities will also form part of the post-event arrangements incorporated into stabilisation, continuity and recovery plans (refer to Clause 7.9).

Communications and consultation should be undertaken with an understanding of how perception of risk can influence judgment and alter the value of information that is provided.

DRAFT

SECTION 12 ACTIVATION AND DEPLOYMENT

Following commencement of a potentially disruptive event, there are a range of actions that should be considered in order to determine whether and when to activate and deploy the plan(s), including—

- (a) assessing the incident—
 - (i) what has happened and how did it occur;
 - (ii) what impacts and new risks have been created;
 - (iii) what parts of the organization and which stakeholders have been or could be affected;
 - (iv) what is the anticipated duration of the incident and its impacts; and
 - (v) whether the event can be managed by routine management arrangements,
- (b) evaluating the incident assessment against activation criteria for each of the plans;
- (c) declaring an incident and activating the plan(s) when activation criteria have been met;
- (d) establishing the critical incident management team and teams identified in other plans for stabilization, continuity and recovery activities;
- (e) establishing and running the incident operations centre (IOC);
- (f) prioritizing issues and activities to be undertaken in managing the incident and its impacts;
- (g) developing a real time incident management plan, based on the prioritization, to guide the initial decision making and activities required to manage the incident;
- (h) controlling and coordinating all activated plans;
- (i) establishing the critical incident management team and teams identified in other plans for stabilization, continuity and recovery activities;
- (j) activating or establishing alternate sites for the restoration of IT or other critical infrastructure capability and for the temporary operation of critical business functions;
- (k) monitoring the incident as it progresses;
- (l) reviewing and adapting plans in response to changing circumstances;
- (m) de-escalating and stepping-down of plans and return to routine management as sustainable capability is re-established;
- (n) conducting a debrief and identifying learning opportunities; and
- (o) ensuring good governance and collation and security of documentation generated during the management and recovery from the incident.

*** END OF DRAFT ***

PREPARATION OF JOINT AUSTRALIAN/NEW ZEALAND STANDARDS

Joint Australian/New Zealand Standards are prepared by a consensus process involving representatives nominated by organizations in both countries drawn from all major interests associated with the subject. Australian/New Zealand Standards may be derived from existing industry Standards, from established international Standards and practices or may be developed within a Standards Australia, Standards New Zealand or joint technical committee.

During the development process, Australian/New Zealand Standards are made available in draft form in order that all interests concerned with the application of a proposed Standard are given the opportunity to submit views on the requirements to be included. Copies of this draft are available through the National Sales Centre, free call 1300 65 46 46.

The following interests are represented on the committee responsible for this draft Australian/ New Zealand Standard:

Australian Computer Society
Australian Council of Trade Unions
Committee IT-012
Committee QR-005
Department of Education and Early Childhood Development Victoria
Emergency Management Australia
Engineers Australia
Environmental Risk Management Authority New Zealand
Financial Services Institute of Australia
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
The Institute of Internal Auditors - Australia
The University of New South Wales

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.co.nz

www.standards.com.au