

COMMITTEE OB-007

DR 09053 CP

(Project ID: 8882)

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 1: Specification**



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 1: Specification

(To be AS/NZS 5050.1:200X)

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.

The objective of this Standard is to provide a structure for a business continuity management system (BCMS).

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 (This Standard)
- 5050.2 Part 2: Practice
- 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.

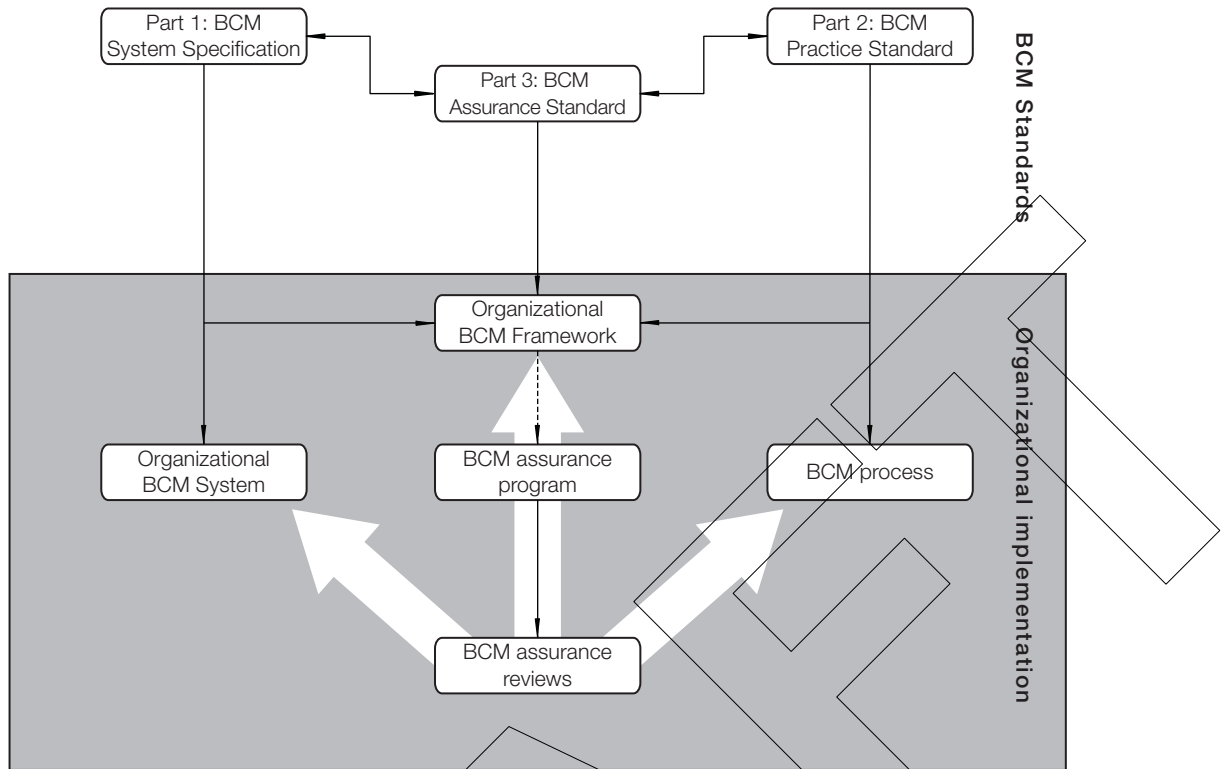


FIGURE P1 BCM STANDARDS' RELATIONSHIPS AND THEIR IMPLEMENTATION

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.

DRAFT

CONTENTS

| | <i>Page</i> |
|--|-------------|
| SECTION 1 SCOPE AND GENERAL | |
| 1.1 SCOPE..... | 5 |
| 1.2 REFERENCED DOCUMENTS..... | 5 |
| 1.3 TERMS AND DEFINITIONS | 5 |
| SECTION 2 THE BUSINESS CONTINUITY MANAGEMENT SYSTEM | |
| 2.1 GENERAL..... | 9 |
| 2.2 GENERAL REQUIREMENTS..... | 9 |
| SECTION 3 PLANNING AND ESTABLISHING THE BCMS FRAMEWORK | |
| 3.1 POLICY..... | 11 |
| 3.2 PLANNING..... | 11 |
| 3.3 ESTABLISHING UNDERSTANDING AND THE FRAMEWORK..... | 11 |
| SECTION 4 ESTABLISHING AWARENESS, UNDERSTANDING AND COMMITMENT | |
| 4.1 GENERAL..... | 13 |
| 4.2 MANAGEMENT COMMITMENT..... | 13 |
| SECTION 5 RISK ASSESSMENT | 14 |
| SECTION 6 BUSINESS IMPACT ANALYSIS..... | 15 |
| SECTION 7 DEVELOPING TREATMENT STRATEGIES..... | 16 |
| SECTION 8 IMPLEMENTATION AND OPERATION | |
| 8.1 IMPLEMENTING TREATMENTS..... | 17 |
| 8.2 COMMUNICATIONS DURING AN EVENT..... | 17 |
| 8.3 DEVELOPING BCM PLANS..... | 17 |
| 8.4 DOCUMENTATION AND ITS CONTROL | 18 |
| 8.5 ACTIVATION AND DEPLOYMENT..... | 18 |
| 8.6 PERFORMANCE ASSESSMENT | 18 |
| SECTION 9 MONITORING AND REVIEW | |
| 9.1 GENERAL..... | 19 |
| 9.2 MANAGEMENT REVIEW..... | 19 |
| SECTION 10 MAINTENANCE AND IMPROVEMENT | |
| 10.1 MAINTENANCE PROCESSES | 20 |
| 10.2 MAINTAINING UNDERSTANDING | 20 |
| 10.3 EXERCISING..... | 20 |
| 10.4 IMPROVEMENT | 20 |
| APPENDIX A STRUCTURE OF THIS STANDARD | 21 |

STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Australian/New Zealand Standard
Business continuity—Managing disruption related risk**Part 1: Specification**

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE

This Standard provides a structure for a business continuity management system (BCMS). The BCMS specifies requirements for developing and implementing policy, frameworks and programs to assist an organization to manage risk arising from business disruption and therefore make it more likely that the organization will achieve its objectives despite disruptive events whether these are within or outside the organization.

This Standard is applicable to any organization that wishes to develop, implement, establish and maintain a BCMS, or requires third party certification of its approach to business continuity management.

The requirements described in this Standard are designed to enable the BCMS to be integrated into an organization's other management systems. As such the elements of the BCMS described in this Standard are in a style and manner that is consistent with other system management Standards, and with the structure presented in ISO Guide 72.

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.

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

1.2 REFERENCED DOCUMENTS

The following documents have been referenced in this Standard.

| | |
|-------------------|---|
| ISO 31000:2009 | Risk Management—Principles and guidelines on implementation |
| Guide 72 | Guidelines for the justification and development of management system standards |

1.3 TERMS AND DEFINITIONS

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

1.3.1 Activation

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

1.3.2 Business continuity management context

A description of the organizational objectives, the parameters both within and outside the organization within which its goals are pursued, the organization's risk tolerance and the stakeholders relevant to achieving business continuity.

1.3.3 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 and information and processes.

1.3.4 Business continuity management system (BCMS)

An overall management system, whether standalone or integrated into the general management system that establishes policy and objectives for business continuity management and provides the means to achieve those objectives.

1.3.5 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.

1.3.6 Capability

Comprises the—

- (a) ability (experience, knowledge, skills, etc of people and organizations, including the ability and fitness for purpose of processes, assets, infrastructure, etc) to undertake the desired activities and achieve required outcomes; and
- (b) capacity (the availability of and access to people, resources, time, space, processes).

1.3.7 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.

1.3.8 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.

1.3.9 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.

1.3.10 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 requires a significant and coordinated urgent response.

1.3.11 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'.

1.3.12 External context

External environment in which the organization seeks to achieve its objectives

NOTE: External context can include—

- (a) the cultural, political, 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) relationships with and perceptions and values of external stakeholders.

1.3.13 Hazard

Source of potential harm

NOTE: A hazard can be a risk source.

1.3.14 Incident response

The sum of the actions taken in response to a disruptive event in order to reduce the consequences and return the organization to its desired or intended recovery position.

1.3.15 Internal context

Internal environment in which the organization seeks to achieve its objectives

NOTE: Internal context can include—

- (a) the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- (b) information systems, information flows, and decision making processes (both formal and informal);
- (c) internal stakeholders;
- (d) policies, objectives, and the strategies that are in place to achieve them;
- (e) perceptions, values and culture;
- (f) standards and reference models adopted by the organization; and
- (g) structures (e.g. governance, roles and accountabilities).

1.3.16 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).

1.3.17 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).

1.3.18 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.

1.3.19 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 (including changes in circumstances), and the associated likelihood of occurrence.

1.3.20 Risk criteria

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

NOTE: Risk criteria are based on organizational objectives and internal and external context. Risk criteria can be derived from Standards, laws, policies and other requirements.

1.3.21 Through chain

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

1.3.22 Vulnerability

Intrinsic properties of something that results in susceptibility to a risk source that can lead to a consequence.

SECTION 2 THE BUSINESS CONTINUITY MANAGEMENT SYSTEM

2.1 GENERAL

The BCMS is a set of governance and strategic requirements, practices, processes, structures, controls, resources and other capabilities that enable an organization to manage disruption risk, respond to events, help to ensure continuity and facilitate recovery. The BCMS can also be an important means of complying with regulatory requirements and satisfying the needs of key stakeholders.

The BCMS provides a structured and repeatable process that assist organizations to minimize or avoid disruption thereby preserving continuity of product or service, and continuing to achieve their critical business objectives

2.2 GENERAL REQUIREMENTS

The organization shall design, develop, implement, document, maintain and continuously improve a business continuity management system that is in accordance with the requirements of this Standard.

The BCMS is based upon the Plan-Do-Check-Act (PDCA) cycle in line with management system standards developed by the International Standards Organization (ISO). The PDCA is one of two approaches to management system standards described in ISO Guide 72, the other is the 'process approach'. Management systems standards generally show a number of common features, comprising—

- (a) policy;
- (b) planning;
- (c) implementation and operation;
- (d) performance assessment;
- (e) improvement; and
- (f) management review.

The key elements of the PDCA management system approach are—

- (i) *Plan*—assessing disruption-related risk in order to understand the organizations strengths and vulnerabilities, how its objectives interact with its internal and external environment, and to determine whether and how the risk needs treating in order to increase the likelihood of achieving those objectives
- (ii) *Do*—implementing the requirements (i.e. risk treatments) developed under 'plan' above;
- (iii) *Check*—monitoring and reviewing both the inputs to the risk assessment, progress made with implementation of risk treatments and the ongoing readiness and relevance of the resulting controls; and
- (iv) *Act*—undertaking any necessary corrections and improvements to the management system, based upon the outputs of 'check' above.

The PDCA cycle for the BCMS is illustrated in Figure 1. It is important to note that the BCMS is an iterative process, and a PDCA cycle occurs as part of each of the stages of the BCMS.

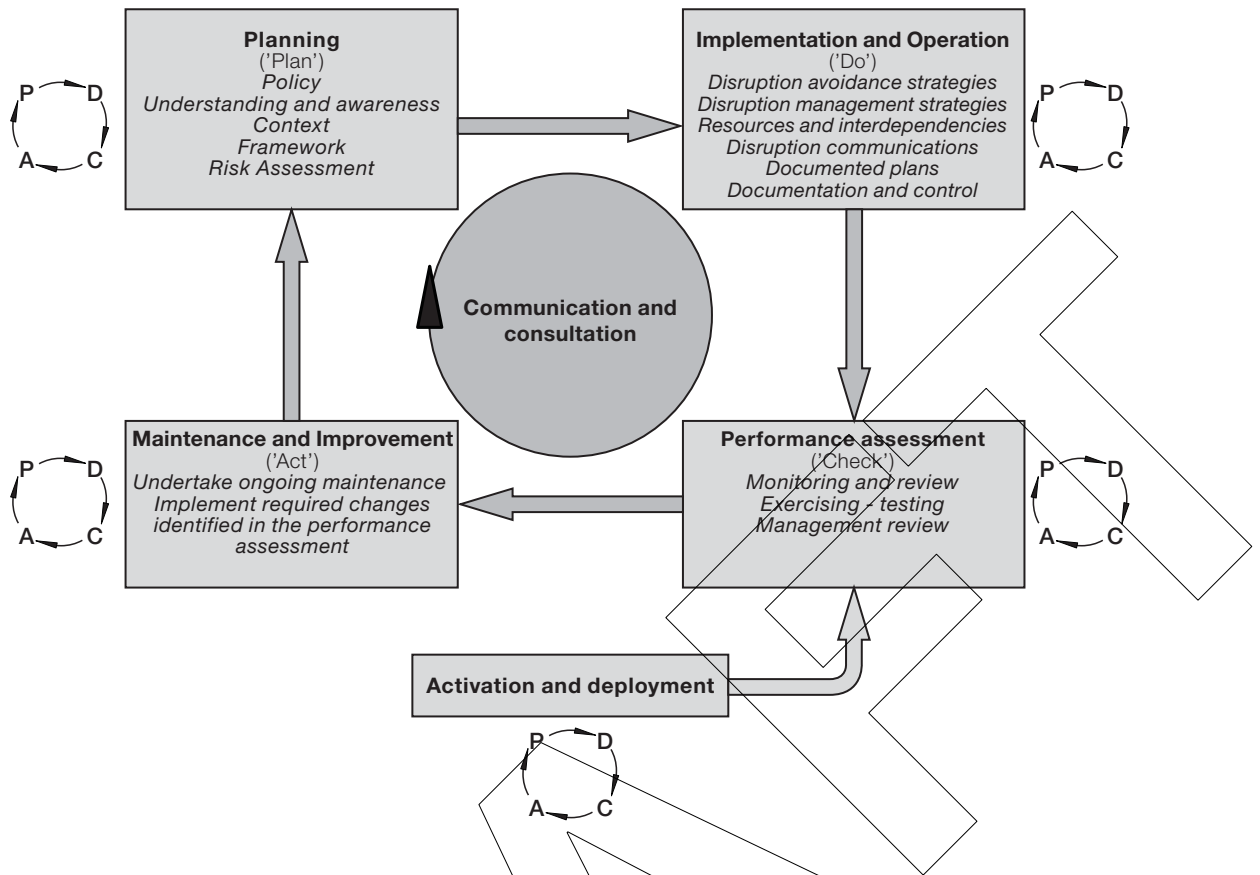


FIGURE 1 THE BCMS CYCLE

SECTION 3 PLANNING AND ESTABLISHING THE BCMS FRAMEWORK

3.1 POLICY

The organization shall develop, document, promulgate and implement a policy for the business continuity management system.

The policy shall—

- (a) be established and approved by the organization's senior management;
- (b) be made available to all employees and contractors of the organization;
- (c) be a controlled document and be subject to regular review and approval;
- (d) provide direction on the objectives, scope and structure for the BCMS;
- (e) identify any authorities and delegations required under the BCMS;
- (f) define roles and responsibilities for the BCMS; and
- (g) promote the need for continuous improvement of the BCMS.

3.2 PLANNING

The organization shall develop and document its plan for the establishment, conduct and integration of BCM arrangements including improvement of any existing arrangements. The planning process shall include the consideration of the design and development of a BCM framework within which the assessment and treatment of disruption related risks will take place.

3.3 ESTABLISHING UNDERSTANDING AND THE FRAMEWORK

3.3.1 General

Where the existing risk management framework does not ensure appropriate understanding of BCMS concepts and organizational requirements the organization shall undertake the development of the context to inform the establishment of the BCMS framework. Particular attention should be given when defining the context to those internal and external factors (including organizational functions, resources and external dependencies) which are most critical to achieving the objectives. These shall be approved by the appropriate authority.

3.3.2 Establishing the context

The organization shall define its risk management context that includes consideration of the—

- (a) the organization's objectives;
- (b) the external context;
- (c) the internal context;
- (d) its risk criteria;
- (e) key business continuity stakeholders; and
- (f) critical drivers for the BCMS.

3.3.3 Adapting the governance and management frameworks of the organization

The organization shall ensure that its governance and management frameworks support the following components of the BCMS:

- (a) A BCMS scope.
- (b) A BCMS policy.
- (c) A business case for the BCMS project (e.g. for the establishment of the BCMS) and program (for the ongoing operation of the BCMS).
- (d) Project/program development and implementation plan for the BCMS, including objectives, schedules and targets.
- (e) Planning, capability development and capability improvement processes.
- (f) BCMS governance and reporting mechanisms.
- (g) Infrastructure and resourcing.
- (h) Individual and team responsibilities and capabilities.
- (i) Consultation and communication strategy and processes.
- (j) Monitoring, review and assurance mechanisms.
- (k) Incident response management.

3.3.4 Legal requirements

The organization shall ensure compliance of the BCMS legislative, regulatory, contractual and other legal requirements.

3.3.5 Documentation requirements

The BCMS shall be supported by documentation that includes—

- (a) documented scopes, policies and procedures;
- (b) documented plans and records; and
- (c) documented assessments and reports

3.3.6 Control of documentation

Documentation shall be controlled according to agreed written document control procedures. Such procedures should include—

- (a) identified responsibilities for the drafting, approval and review of the documents;
- (b) timelines for review and revision of documents;
- (c) mechanisms for identifying changes and version control;
- (d) controls for distribution of the documents;
- (e) identifiable access approvals and audit trails;
- (f) requirements for storage;
- (g) requirements for the disposal of obsolete documents; and
- (h) mechanisms for the backup of documents.

SECTION 4 ESTABLISHING AWARENESS, UNDERSTANDING AND COMMITMENT

4.1 GENERAL

The organization shall where necessary, undertake formal development, engagement and communication activities to improve the awareness of employees, contractors and partners regarding the BCMS and the organization's need for it.

The organization shall identify those individuals that require a more detailed understanding of the BCMS and develop awareness and training activities to promote that understanding. These may include verbal, written and electronic communications covering the following topics:

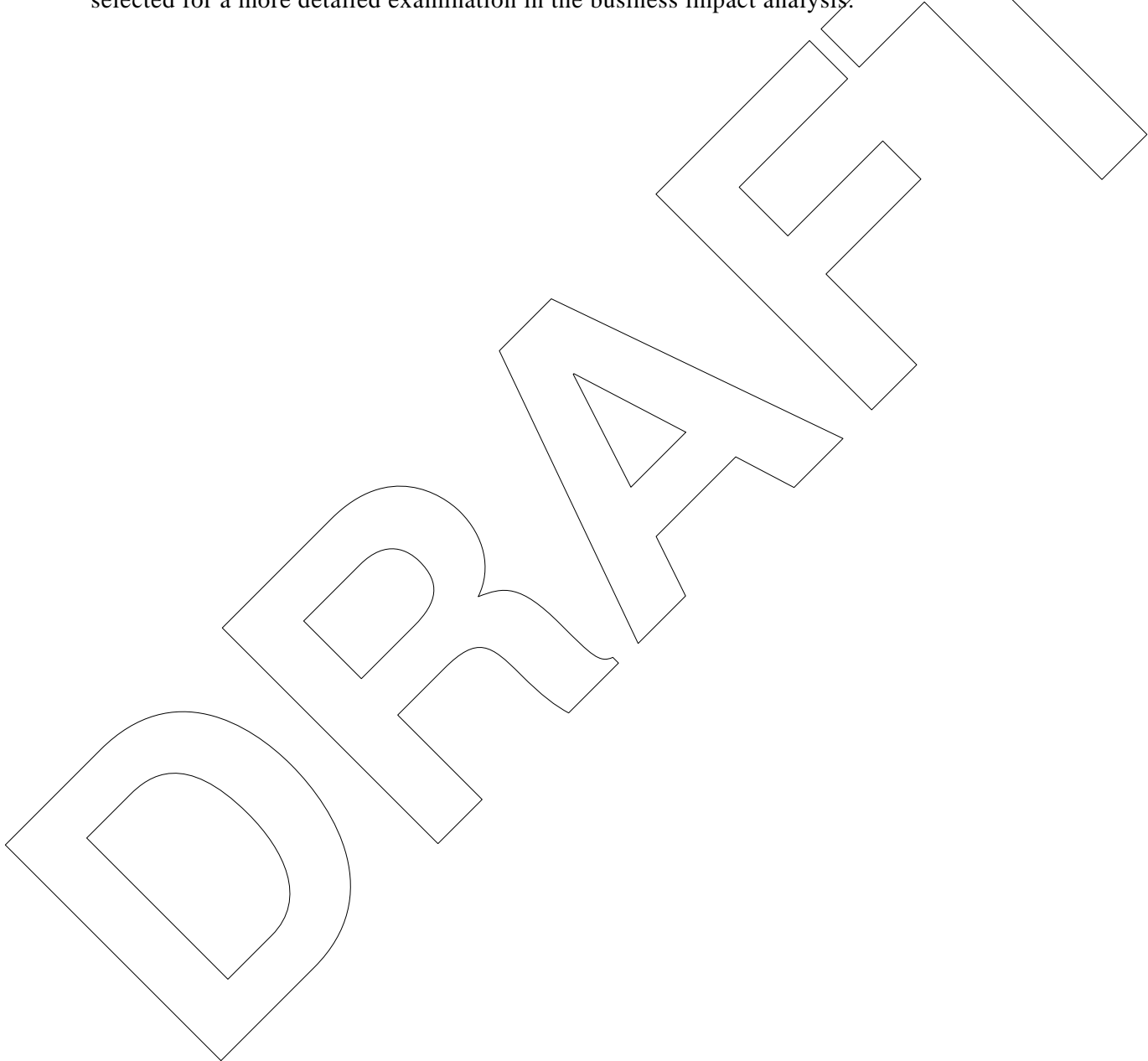
- (a) A conceptual overview of the BCMS and its role within the organization's overall risk management approach.
- (b) The organizational need for the BCMS.
- (c) The composition, structure, framework, processes involved in the BCMS.
- (d) The benefits the organization is expected to derive from the BCMS.
- (e) Potential resource implications of implementing the BCMS.
- (f) Roles and responsibilities within the BCMS.

4.2 MANAGEMENT COMMITMENT

Management shall provide evidence that its commitment to the BCMS is commensurate with its BCMS objectives and that the necessary resources are provided to achieve those objectives.

SECTION 5 RISK ASSESSMENT

The organization shall undertake an assessment of disruption related risks, involving the identification, analysis (including business impact analysis) and evaluation of those risks. The organization shall use risk assessment techniques that are robust, documented and appropriate. The risk assessment should consider sources of risks and the performance of any controls in relation to those risks and compare the level of risk with the organization's risk criteria (which will reflect the organization's appetite for risk) in order to determine the need for and priority of risk treatments. Those risks that exceed the risk criteria should be selected for a more detailed examination in the business impact analysis.



SECTION 6 BUSINESS IMPACT ANALYSIS

Analysis should be made of the impacts (consequences) of disruption-related risks on the critical business functions or other critical elements over a range of defined time periods following the onset of the disruptive event. These critical elements include processes, systems, information, people, assets and other dependencies both inside and outside the organization. .

The risk criteria against which disruption-related risks are evaluated should consider the sensitivities of each critical business function to different types of disruption and the maximum acceptable outage times for those functions.

In considering existing controls, the analysis should consider both those that affect the likelihood of disruptive events and those which relate to the organization's current capacity and preparedness to respond to and manage the impacts of disruption, having regard to—

- (a) dependencies which may be affected by disruption;
- (b) the minimum resources likely to be required to ensure that critical business functions continue to operate at the level required to achieve the critical objectives; and
- (c) the availability of potential workarounds, which could reduce disruption.

SECTION 7 DEVELOPING TREATMENT STRATEGIES

If the risk evaluation shows a need to reduce or otherwise treat the risk, the organization shall identify, as appropriate, options for reducing the likelihood of disruptive events and or reducing the impact through preparedness, stabilization, continuity and recovery. The organization should therefore consider treatments such as—

- (a) avoiding the circumstances that can either cause or make the organization vulnerable to disruptive events;
- (b) taking measures to reduce the likelihood of disruptive events;
- (c) reducing the impact (consequences) of events (or the likelihood of those consequences arising), by reducing the scale or duration of loss and harm, including sharing the risk (for example through insurance); and
- (d) increasing the duration and likelihood of exposure to, or uptake of, beneficial consequences.

These treatments may be developed through considering strategies such as—

- (i) improving prevention and protection measures that will lessen the likelihood, magnitude or duration of events which can cause disruption;
- (ii) establishing alternate processes;
- (ii) creating redundancy in processes;
- (iii) creating redundancy in inventory;
- (iv) enhancing people capabilities, including multi-skilling of key staff;
- (v) creating access to additional people capability through outsourcing;
- (vi) establishing mutual aid agreements with external organizations to provide temporary access to additional capability;
- (vii) strengthening relationships with key stakeholders; and
- (viii) identifying alternate logistics solutions.

The organization should conduct a cost benefit analysis to determine the most appropriate treatments, identify any new interdependencies that would be created by the selected treatments and consider whether these create further risks that will require assessment and possible treatment.

SECTION 8 IMPLEMENTATION AND OPERATION

8.1 IMPLEMENTING TREATMENTS

The organization shall determine, allocate and if necessary prioritize the resources and capabilities needed to implement the selected risk treatments. This includes those resources capabilities required to be established pre-event (as part of preparedness) as well as arrangements for acquiring or accessing resources and capabilities that will be required during and post event, for stabilization, continuity and recovery.

The following types of resources should be considered:

- (a) People.
- (b) Information and data.
- (c) Facilities and equipment.
- (d) IT and telecommunications systems.
- (e) Transportation.
- (f) Finances.
- (g) Other assets and consumables.
- (h) Critical infrastructure access and availability.
- (i) Third party suppliers and contractors.

8.2 COMMUNICATIONS DURING AN EVENT

Where the selected treatments envisage special forms of communication with stakeholders, the community or others during the period of disruption, planning for such communications should consider—

- (a) aims, objectives and scope of communications;
- (b) preparation of communication plans and templates;
- (c) authorities for approval and release of communications;
- (d) mechanisms for distribution of the communications; and
- (e) arrangements to monitor and review the effectiveness of the communications.

8.3 DEVELOPING BCM PLANS

Plans which address preparedness, stabilization, continuity and recovery requirements shall be recorded.

Such plans shall be to a sufficient level of complexity having regard to the knowledge and skills of those who will use them. The organization should consider what type and number of plans should be developed to address the range of critical business functions and geographical locations that have been identified.

Plans shall consider the requirements for—

- (a) initially responding to an incident, assessing the incident and managing any immediate threats, harm or loss to people, property and information;
- (b) ensuring the organization will have a minimal acceptable capability to achieve its critical objectives; and

- (c) recovering from the effects of disruption and achieving the recovery objectives

8.4 DOCUMENTATION AND ITS CONTROL

The organization shall ensure that its risk management documentation includes the information and data that is essential to the successful implementation and management of the BCMS, and that there are processes for its control, including preparation, approval, finalization, dissemination, storage, retrieval, protection, review, revision and disposal.

8.5 ACTIVATION AND DEPLOYMENT

The organization shall have documented plans and procedures that will be implemented should predetermined activation criteria be met. The organization should assess the incident and then develop a detailed incident management plan based upon this assessment and relevant requirements of the BCMS plans already in place. The incident management plan should identify specific responsibilities and actions to be undertaken.

8.6 PERFORMANCE ASSESSMENT

The organization shall ensure that its risk management assurance arrangements extend to and include monitoring and review of all matters covered by the BCMS as well as periodic review of the BCMS itself.

The organization shall implement procedures to assess the performance of the BCMS to ensure the ongoing reliability of active BCM controls. Many of these controls require ongoing support activities in order for them to be able to be relied upon for their intended effect.

SECTION 9 MONITORING AND REVIEW

9.1 GENERAL

The organization's monitoring and review activities should inform and direct process that will maintain the required levels of resources and capabilities, create continuous improvement of the BCMS. The organization should also establish criteria that will trigger additional maintenance and improvement activities in response to changes that have a material impact on the achievement of the organization's objectives.

Assurance activities should be of a type and occur at appropriate intervals that are appropriate to likelihood and nature of change (for example of personnel or aspects of the risk management context) and to the results of previous assurance activities.

Such activities may include—

- (a) self assessment of the BCMS;
- (b) independent audit of the BCMS;
- (c) management review of the BCMS;
- (d) monitoring and review of any changes to the context or risk assessment;
- (e) assessment of the status and effectiveness of treatment strategies;
- (f) assessment of the effectiveness of the status of resources and other capabilities; AND
- (g) exercising of the stabilization, continuity and recovery plans and capabilities developed through the BCMS, to test and evaluate their feasibility, readiness and effectiveness.

The organization should consider the requirements to provide assurance to stakeholders in deciding on which performance assessment activities to undertake.

9.2 MANAGEMENT REVIEW

Reviews of the BCMS, at agreed intervals, should determine its status, performance, ongoing appropriateness, efficiency and effectiveness to meet the documented BCMS scope and objectives. The outcomes from the review may result in—

- (a) revision of the objectives and scope for the BCMS;
- (b) revision of the risk criteria and stakeholders;
- (c) improvement in the structure and performance of the BCMS;
- (d) revision of critical objectives for the organization;
- (e) changes to agreed provision of resources;
- (f) redesign of organizational structures and processes;
- (g) improvements in organizational capability, efficiency and effectiveness; and
- (h) improved compliance with regulatory requirements.

SECTION 10 MAINTENANCE AND IMPROVEMENT

10.1 MAINTENANCE PROCESSES

The organization shall establish, schedule and implement maintenance processes that allow and ensure the BCMS will function as intended.

10.2 MAINTAINING UNDERSTANDING

The organization shall establish processes that allow identified key people (including appropriate internal and external stakeholders) to maintain their understanding of—

- (a) the BCMS;
- (b) the risk management context including critical objectives and vulnerabilities,
- (c) disruption-related risks;
- (d) capabilities of the organization on which business continuity objectives rely; and
- (e) roles and responsibilities.

10.3 EXERCISING

The organization should consider conducting exercises that not only test and evaluate, but will also enhance the plans and capabilities developed under the BCMS. performance of the stabilization, continuity and recovery plans and capabilities, but should a developed under the BCMS. Exercises should be conducted in a manner that allows those with specific functions to practice and perform those functions and (as part of the assurance program) to test the effectiveness of the plan and the required organizational capabilities.

The design, development and conduct of an exercise shall be undertaken using a process that ensures clear objectives are established for the exercise and that the outcomes of the exercise are reviewed against these objectives. The organization shall ensure that key outputs and outcomes arising from, and key decisions undertaken in the design, development, conduct and review of an exercise are documented.

10.4 IMPROVEMENT

10.4.1 Remedial actions and continuous improvement

The organization shall establish and implement ongoing processes that will allow—

- (a) preventive actions to be undertaken to address potential causes of non-conformities;
- (b) corrective actions (including those identified by the monitoring and review arrangements) to be undertaken in response to identified non-conformances; and
- (c) continual improvement in the framework, implementation and operation of the BCMS to be pursued.

APPENDIX A
 STRUCTURE OF THIS STANDARD
 (Informative)

Although this Standard which concerns management of disruption-related risk has been developed in conformity with ISO 31000:2009, its structure is also broadly consistent with the common elements of management system standards (MSS) as presented in ISO Guide 72:2001. Table A1 illustrates the alignment of this Standard with these common elements.

TABLE A1
ALIGNMENT OF THE BCMS SPECIFICATION STANDARD WITH
MSS MAIN SUBJECTS AND COMMON ELEMENTS

| PDCA | MSS main subject and common element | AS/NZS 5050.1—200X element (section #) |
|---|---|---|
| Plan | Policy | Policy (3) |
| | Planning | Planning (3) |
| | Identification of needs, requirements and analysis of critical issues | Establishing understanding and the framework (3, 4, 5, 6) |
| | Selection of significant issues to be addressed | |
| | Setting of identification of resources objectives and targets | |
| | Identification of organizational structure, roles, responsibilities and authorities | |
| | Planning of operational processes | |
| Contingency preparedness for foreseeable events | | |
| Do | Implementation and operation | Implementation and operation: developing capabilities (8) |
| | Management of human resources | Developing and analysing disruption management strategies (7) |
| | Management of other resources | Establishing resources and interdependencies (7, 8) |
| | | Developing documented plans (7, 8) |
| | Documentation and its control | Activation and deployment (7, 8) |
| | Communication | Documentation and its control (7, 8) |
| | Relationship with suppliers and contractors | Developing disruption communications (7, 8) |
| Check | Performance assessment | Establishing resources and interdependencies (7, 8) |
| | Monitoring and measuring | Performance assessment (8) |
| | Analysing and handling nonconformities | Monitoring and review (9) |
| Act | System audits | |
| | Improvement | Improvement (10) |
| | Corrective action | Establishing maintenance activities (10) |
| | Preventive action | Maintaining understanding (10) |
| | Continual improvement | Maintaining performance (10) |
| | Management review | Exercising (10) |
| | | Management review (10) |

*** 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