

COMMITTEE OB-007

DR 09055 CP

(Project ID: 8977)

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 3: Assurance



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

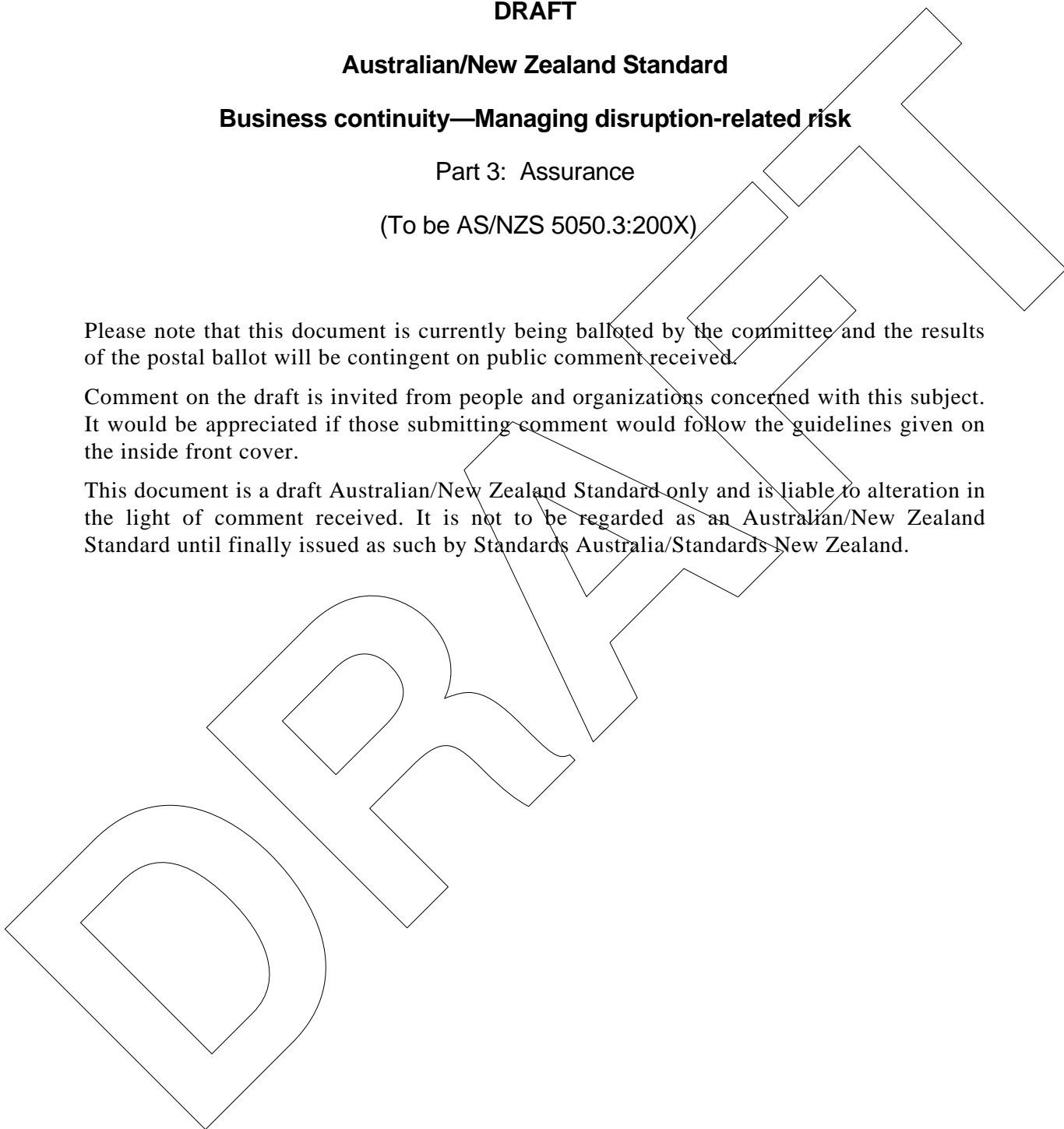
Part 3: Assurance

(To be AS/NZS 5050.3:200X)

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 detail the processes required to enable organizations to develop, implement and conduct an audit and other assurance processes that will assist in determining the ongoing adequacy of an organization's assessment and treatment of disruption-related risk including all controls relating to making potentially disruptive events less likely, and preparing for, responding to and recovering from such incidents.

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
5050.3	Part 3: Assurance (This Standard)

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.

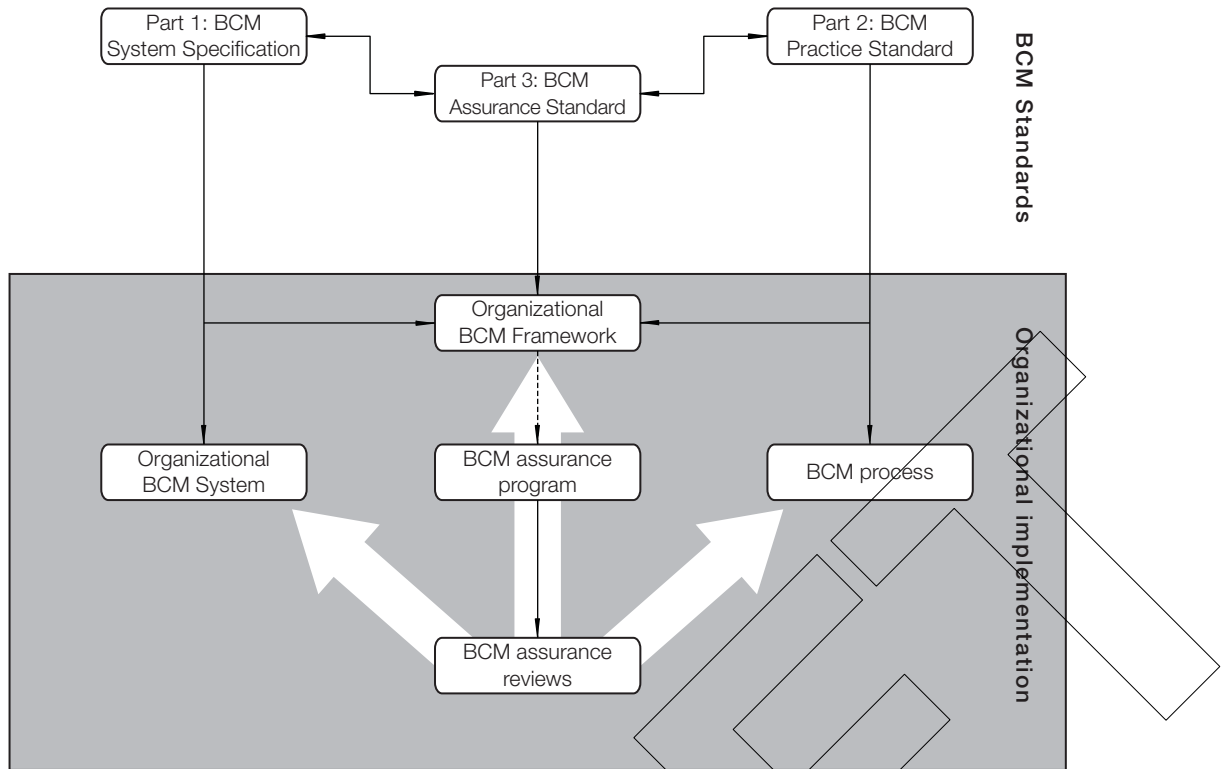


FIGURE P1 BCM STANDARDS' RELATIONSHIPS AND THEIR IMPLEMENTATION

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.

CONTENTS

	<i>Page</i>
SECTION 1 SCOPE AND GENERAL	
1.1 SCOPE AND APPLICATION.....	5
1.2 DEFINITIONS.....	5
1.3 REFERENCED DOCUMENTS.....	6
SECTION 2 ASSURANCE OVERVIEW	
2.1 GENERAL.....	7
SECTION 3 ESTABLISHING THE FRAMEWORK	
3.1 POLICY.....	9
3.2 ARRANGEMENTS.....	9
3.3 FRAMEWORK IMPROVEMENT.....	9
3.4 COMMUNICATIONS.....	9
SECTION 4 DEVELOPING AN ASSURANCE PROGRAM	
4.1 GENERAL.....	10
4.2 DEVELOP THE BCM ASSURANCE PROGRAM SCOPE.....	11
4.3 DEVELOP THE BCM ASSURANCE PROGRAM PLAN.....	11
4.4 ESTABLISH BCM ASSURANCE PROGRAM GOVERNANCE REQUIREMENTS.....	12
4.5 ESTABLISH BCM ASSURANCE PROGRAM RESOURCES.....	12
4.6 IMPLEMENT AND CONDUCT THE BCM ASSURANCE PROGRAM.....	12
4.7 CONDUCT BCM ASSURANCE PROGRAM REVIEW, REPORTING AND IMPROVEMENT.....	13
SECTION 5 DEVELOPING AND CONDUCTING SPECIFIC ASSURANCE REVIEW ACTIVITIES	
5.1 GENERAL.....	14
5.2 DEVELOP THE BCM ASSURANCE REVIEW ACTIVITY SCOPE.....	14
5.3 ESTABLISH AIM AND OBJECTIVES.....	15
5.4 SELECT BCM AREAS TO BE REVIEWED.....	15
5.5 DETERMINE METHODOLOGIES.....	15
5.6 ALLOCATE RESOURCES.....	16
5.7 APPROVE THE SCOPE.....	16
5.8 DEVELOP THE ASSURANCE REVIEW ACTIVITY PLAN.....	16
5.9 IMPLEMENT AND CONDUCT THE REVIEW.....	16
5.10 SUITABILITY OF PROVIDERS.....	17
5.11 REPORTING.....	17
APPENDICES	
A EXAMPLE BCM ASSURANCE REVIEW ACTIVITY SCOPE (HYPOTHETICAL ONLY).....	18
B EXAMPLE BCM ASSURANCE APPROACH.....	19
C EXAMPLE TEMPLATE FOR REVIEW OF THE BCM SYSTEM (ILLUSTRATIVE EXAMPLE ONLY).....	20
D EXAMPLE TEMPLATE FOR A REVIEW OF THE BCM PROGRAM (ILLUSTRATIVE EXAMPLE ONLY).....	23
E EXAMPLE TEMPLATE FOR A REVIEW OF BUSINESS CONTINUITY PLAN (ILLUSTRATIVE ONLY).....	26
F EXAMPLE OF REVIEW AREA WITHIN THE BCM FRAMEWORK (ILLUSTRATIVE EXAMPLE ONLY).....	28

STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Australian/New Zealand Standard
Business continuity—Managing disruption-related risk**Part 3: Assurance**

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE AND APPLICATION

This Standard provides a structure and requirements for the development and implementation of an assurance program (including audit) for monitoring and review of an organisation's Business Continuity Management (BCM) arrangements. The described methodology will assist an organization in measuring and validating the ongoing adequacy of the assessment and treatment of disruption-related risks and the efficacy of related controls, having regard to the organisation's BCM objectives (including any regulatory or other obligations). This Standard is applicable to any organization that—

- (a) seeks to verify, evaluate, measure or assess the ongoing adequacy of the business continuity management system, its component parts or related systems and processes;
- (b) is required to demonstrate conformance with an auditable system;
- (c) requires certification of its approach to business continuity management; and
- (d) seeks to provide assurance to its governance and management bodies of the ongoing adequacy of the business continuity management system.

The process described in this (Part 3) of this Standard can be applied to any type of organization, public, private or not-for-profit, and of any size or complexity.

1.2 DEFINITIONS

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

1.2.1 Assurance

A process involving monitoring and review that increases confidence within acceptable limits of certainty that planned objectives will be achieved.

1.2.2 Assess

To examine something in context, in order to judge or evaluate it.

1.2.3 Audit

A process of systematic review against pre-determined criteria.

External audit: the review is conducted by an independent third party and typically includes formal findings in relation to the review criteria (which may include regulatory obligations).

Internal audit: the review is conducted by members of the organisation who are independent of the functions or responsibilities being audited.

1.2.4 Control

Something that is modifying risk (see Clause 3.1).

NOTES:

- 1 Controls include any process, policy, device, practice, or other actions which modify risk.
- 2 Controls may not always exert the intended or assumed modifying effect

1.2.5 Evaluate

To consider or examine something against criteria in order to determine its acceptability

1.2.6 Measure

To assess the effect or quality of something, often against a Standard.

1.2.7 Verify

To check whether or not something is true by examination, investigation, or comparison.

1.3 REFERENCED DOCUMENTS

The following documents have been referenced in this Standard.

AS/NZS

- 5050 Business continuity—Managing disruption-related risk
- 5050.1 Part 1: Specification
- 5050.2 Part 2: Practice

ISO

- 31000 Risk Management—Principles and guidelines on implementation

SECTION 2 ASSURANCE OVERVIEW

2.1 GENERAL

The goal of a BCM assurance program is to provide ongoing confirmation to those responsible for BCM activities (such as the Board, senior management, and regulators) and, possibly, stakeholders e.g. customers and other dependents) that an organization has the structure, resources and processes in place to that provide the capacity to continue to sufficiently achieve critical objectives, despite occurrence of a disruptive event .

BCM assurance is part of the organisation’s monitoring and review activities associated with managing disruption-related risk. It may be achieved via a standalone program or, more commonly, as part of the organisation’s general assurance arrangements. Standalone arrangements should be designed, structured, resourced and governed within a framework as described at Figure 1.

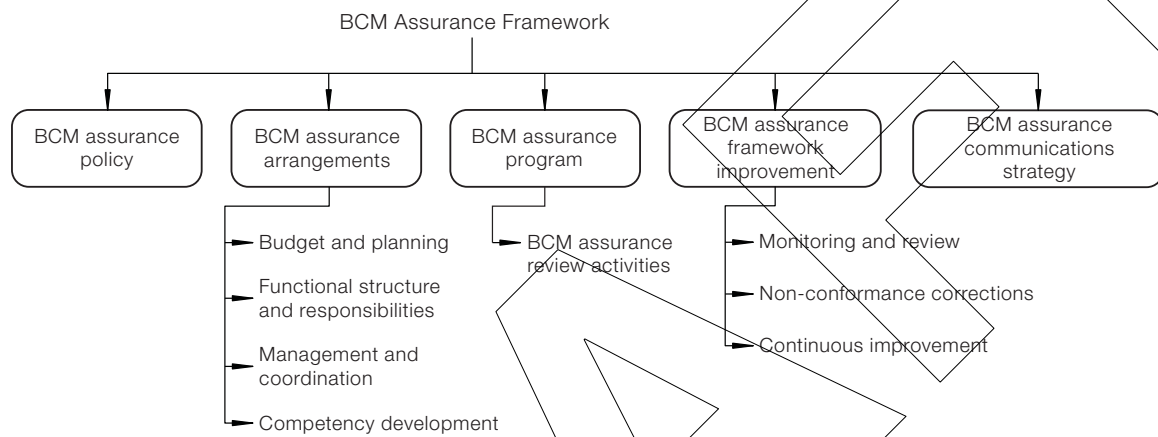


FIGURE 1 EXAMPLE OF A BCM ASSURANCE FRAMEWORK

This framework supports any mix of assurance activities including scheduled reviews, reporting and evaluation of monitoring data and annual audit. This provides for a strategic approach within which a number of individual assurance activities can be conducted over an agreed period of time (see Figure 2).

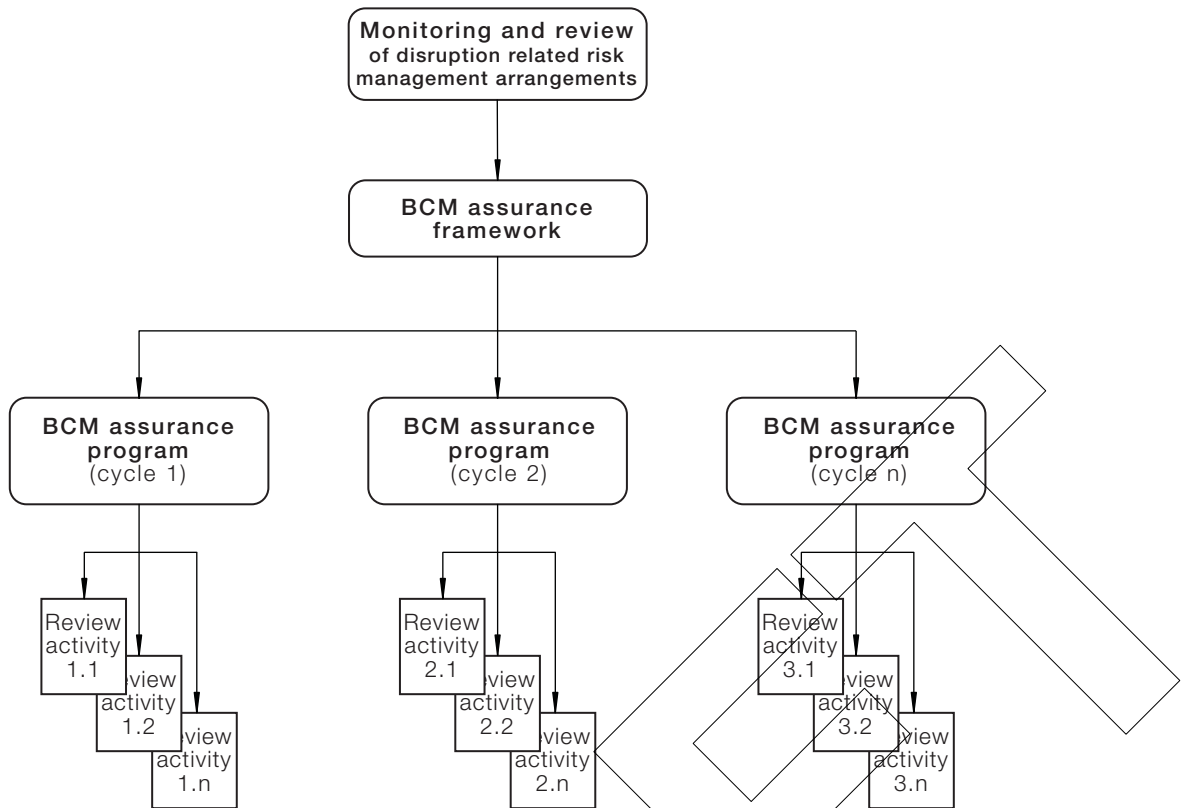


FIGURE 2 ASSURANCE PROGRAM STRUCTURE

Broadly, there are two assurance considerations—

- (a) reviewing capability, performance and compliance against agreed requirements (for example as described in legislation, a standard, organizational policy, or stakeholder agreement); and
- (b) reviewing to identify strengths and weaknesses in the BCM framework and its application. This could include—
 - (i) the effectiveness of controls;
 - (ii) the manner in which the assessment and treatment of risks is undertaken;
 - (iii) the level and clarity of understanding of the purposes and arrangements for BCM by those in the organization required to have such knowledge.

SECTION 3 ESTABLISHING THE FRAMEWORK

3.1 POLICY

The organization's risk management policies should include reference to the need for an assurance framework and program as part of the monitoring and review arrangements. This should apply, inter alia to management of disruption-related risk and therefore the BCM arrangements.

3.2 ARRANGEMENTS

The framework through which BCM assurance is achieved should incorporate—

- (a) a functional structure, that includes responsibilities, accountabilities and resourcing to ensure compliance and coordination;
- (b) procedures for planning and budgeting;
- (c) an approach for continuing the development of competency to be used in deploying and maintaining the framework; and
- (d) systems and process for assisting in the management and coordination of the framework.

3.3 FRAMEWORK IMPROVEMENT

The organization's governance structures, resources and processes should ensure ongoing—

- (a) monitoring and review of the BCM assurance framework;
- (b) corrective actions; and
- (c) continual improvements to the BCM assurance arrangements.

3.4 COMMUNICATIONS

The organization should develop and implement a communications strategy ensuring that—

- (a) all key internal and external stakeholders receive information regarding the BCM assurance framework relevant to their role; and
- (b) consideration is given to promoting awareness and education regarding the assurance program; and

SECTION 4 DEVELOPING AN ASSURANCE PROGRAM

4.1 GENERAL

The assurance program for BCM arrangements should provide for a range of assurance activities to be conducted over a defined period. The time period selected should be appropriate to its purpose (for example to conform with the organisation’s risk management policy, or to fulfil regulatory requirements or contractual obligations) and should have regard to the organisational context (for example, the prevalence of change and past experience). For most circumstances an annual assurance cycle may be appropriate, with a number of assurance activities or reviews scheduled to be undertaken for the whole or parts of the BCM framework, across the whole or parts of the organization (such as different geographical locations, sites, critical business functions). The key elements of an assurance program are illustrated in Figure 3.

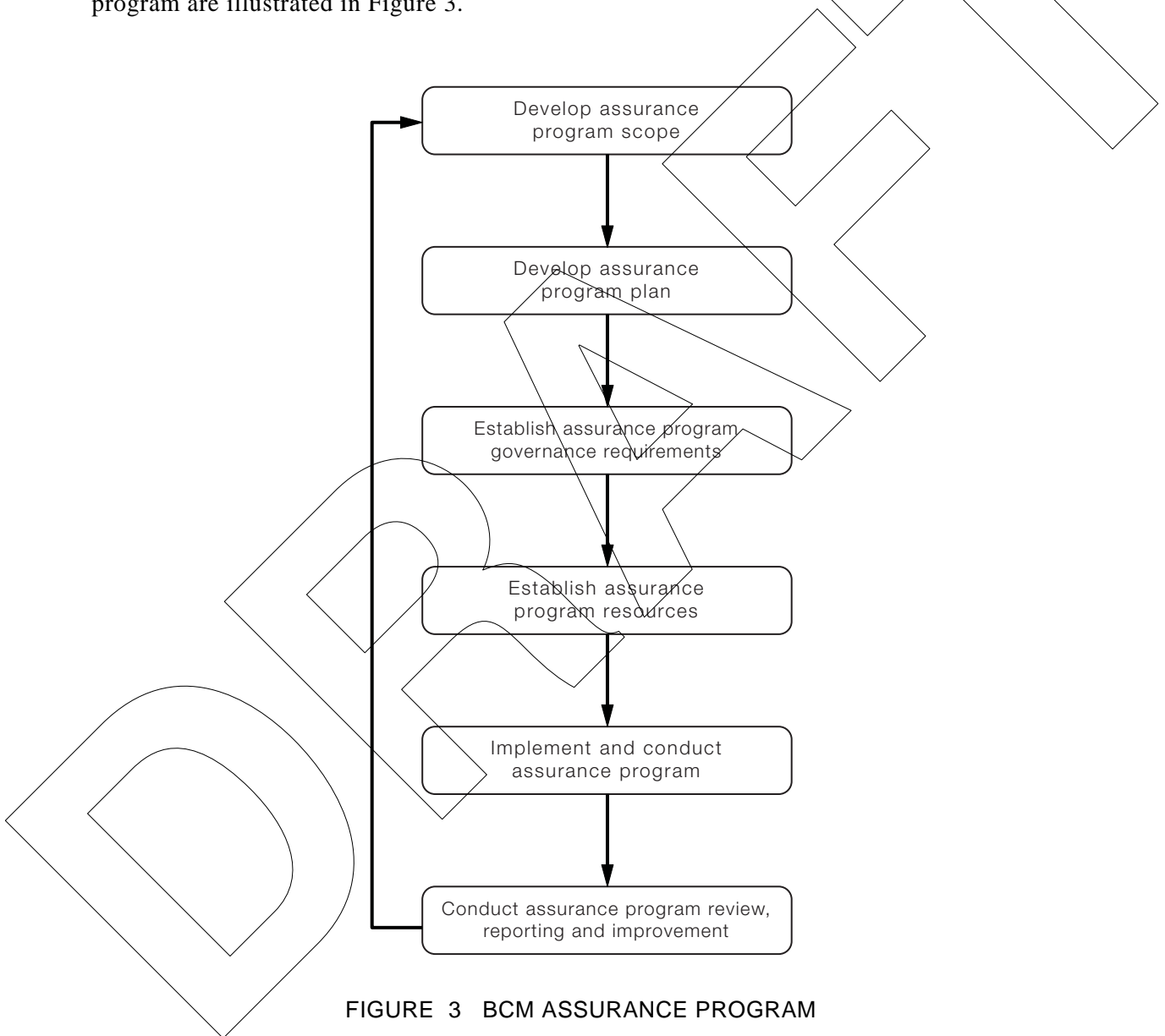


FIGURE 3 BCM ASSURANCE PROGRAM

4.2 DEVELOP THE BCM ASSURANCE PROGRAM SCOPE

4.2.1 Elements

A scope for the BCM assurance program should be developed. This scope should identify—

- (a) the aim and objectives for the BCM assurance program;
- (b) the time period over which the assurance activities will be conducted;
- (c) the requirements (based on the objectives and aims) for conducting the assurance program over the defined time period;
- (d) the parts of the BCM framework that will be examined during the current cycle of the program;
- (e) budget available for conducting the assurance program;
- (f) the processes that will be employed and be available for undertaking assurance activities;
- (g) the areas within the organization that will be examined; and
- (h) measurable performance criteria that will be adopted.

4.2.2 Prioritization of the scope

It is possible that the scoping exercise will identify a far greater range of assurance opportunities than the organization has the resources and time to undertake. It is therefore important that the proposed assurance activities are appropriately prioritized and their boundaries of inclusion and exclusion are defined. Decisions on prioritization of assurance activities should be based upon defined criteria such as—

- (a) determination of a mandatory requirement to examine an area, function, capability;
- (b) evidence of prior material control failures and near misses;
- (c) evidence of current existing material control weakness;
- (d) potential for future material control failure or weakness;
- (e) identified risks relating to the structure, resourcing or capability of the BCMS, or BCM program;
- (f) areas, activities, capabilities, that have been, are, or may be subject to change; and
- (g) perceived need to improve efficiency and effectiveness.

4.3 DEVELOP THE BCM ASSURANCE PROGRAM PLAN

A plan should be developed for each cycle of the BCM assurance program (for example annually). The assurance program plan is developed according to the scope, aim and objectives and should identify the following:

- (a) Individual assurance activities to be undertaken.
- (b) A schedule for the commencement and completion of each assurance activity.
- (c) Resources to be allocated to undertake each activity (including in-house and outsourced resources where appropriate).
- (d) Reporting requirements and milestones for each activity, such as—
 - (i) dates for the presentation of draft report(s) with recommendations;
 - (ii) dates for the receipt of any management response to the recommendations and for finalization of the report(s); and

- (iii) dates for presentation of the final report to the appropriate persons or organisations.

The draft plan should be subject to review and approval by an appropriate authority prior to finalization (refer to Clause 4.4).

4.4 ESTABLISH BCM ASSURANCE PROGRAM GOVERNANCE REQUIREMENTS

The requirements and structure for governance of the BCM assurance program should be established. This should include consideration of the following:

- (a) The identity of those individuals or groups tasked with authorizing and approving the—
 - (i) structure and scope of the BCM assurance program;
 - (ii) content and projected deliverables of the BCM assurance program plan;
 - (iii) resources allocated to the conduct of the program; and
 - (iv) final reports;
- (b) The level of management required to finalize and approve any management comments to recommendations issued in assurance reports.
- (c) Other requirements for reporting on the outcomes of assurance (for example regulatory and contractual reporting requirements).

4.5 ESTABLISH BCM ASSURANCE PROGRAM RESOURCES

The organization should determine and establish those resources that will be required for the efficient and effective development and delivery of the BCM assurance program. These resources should be identified in the assurance program plan and could include—

- (a) in-house and outsourced assurance specialists (including auditors);
- (b) in-house or outsourced subject matter experts (for example ICT technical expertise);
- (c) administrative support;
- (d) training
- (e) program budget;
- (f) assurance software applications; and
- (g) accommodation, consumables, computing and other equipment requirements.

4.6 IMPLEMENT AND CONDUCT THE BCM ASSURANCE PROGRAM

The program should be conducted according to the agreed and approved BCM assurance program plan. Any variations to this plan should be subject to approval as determined in the program governance arrangements.

Each of the approved monitoring and review activities should be undertaken using a robust documented process. One approach to this is described in Section 5.

4.7 CONDUCT BCM ASSURANCE PROGRAM REVIEW, REPORTING AND IMPROVEMENT

4.7.1 Key performance indicators

The BCM assurance program should be reviewed on a regular basis. The frequency for this depends upon the context applying to each individual organization. The review should be based on identified key performance indicators which could include the following:

- (a) *Timeliness*—performance of the program against the activity schedule identified in the BCM assurance program plan.
- (b) *Quality*—performance of the program, generally measured as a result of feedback received from areas subject to review and monitoring activities and from the recipients of the outcomes (for example review reports) and is often based upon—
 - (i) the manner in which the program is conducted;
 - (ii) the breadth and depth of findings made; and
 - (iii) the relevance and usefulness of recommendations made;
- (c) *Cost*—actual expenditure measured against projected budget and against the value received from the BCM assurance program.

4.7.2 Reporting

A regular report on the conduct of the assurance program should be provided to appropriate authorities at regular agreed times. The report should provide information on the following:

- (a) Status of the assurance plan, including—
 - (i) items closed since the last report, the proposed and actual completion dates identified;
 - (ii) new items appearing in the report for the first time, with proposed completion date;
 - (iii) items due for closure, but not yet completed, accompanied with an explanation and a recommended new deadline;
 - (iv) items not yet due for closure, with the proposed completion date identified; and
 - (v) explanation of any delays in the program plan encountered.
- (b) A summary of the outcomes of each of the program reviews completed to date.
- (c) Status of corrections or resolutions of non-compliances or other recommendations made on individual assurance activities.
- (d) The identification and status of improvement actions based upon the measured performance of the BCM assurance program.

SECTION 5 DEVELOPING AND CONDUCTING SPECIFIC ASSURANCE REVIEW ACTIVITIES

5.1 GENERAL

Based upon the assurance program plan, a schedule of individual assurance review activities should be developed. The organization should have in place a documented process for undertaking the development and conduct of each of these individual reviews. An approach to undertaking an individual assurance review activity is described in Figure 4.

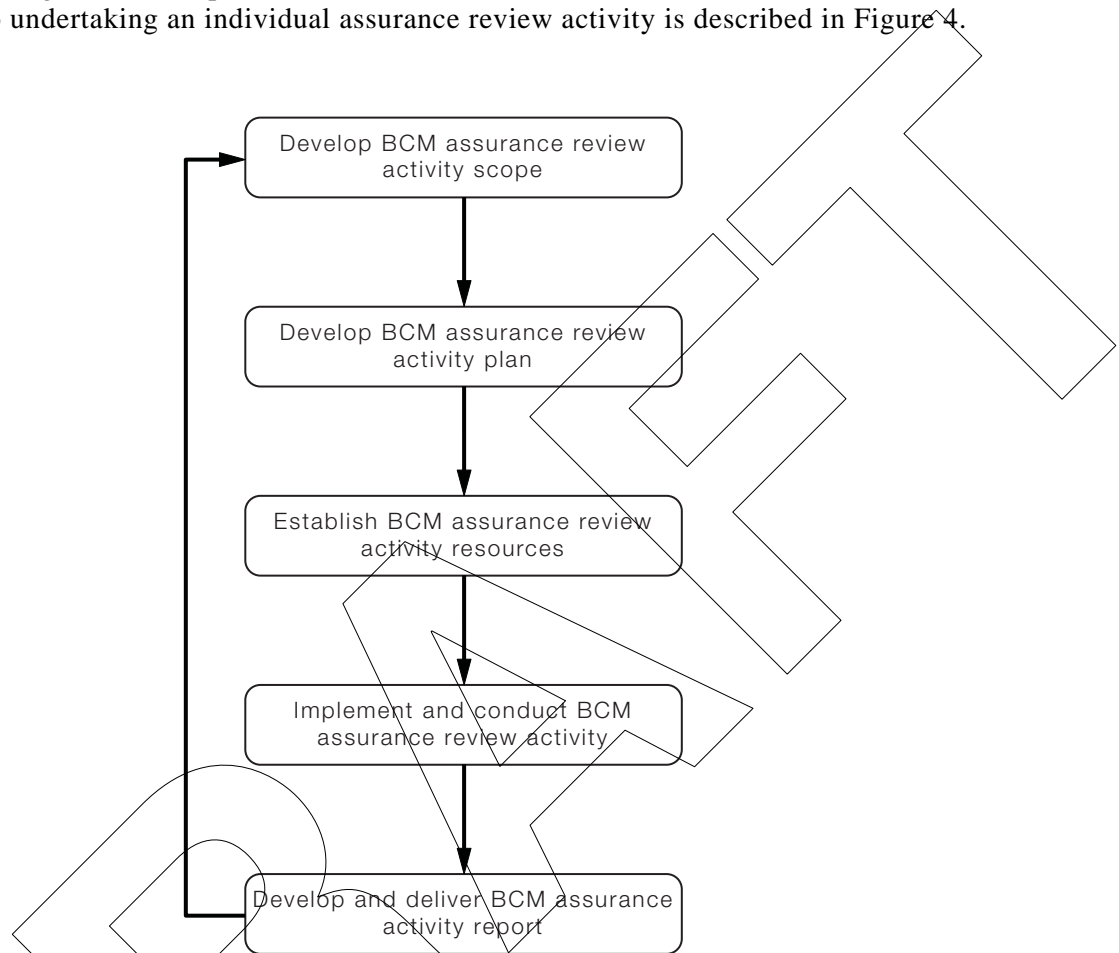


FIGURE 4 PROCESS FOR DEVELOPING AND CONDUCTING A BCM ASSURANCE REVIEW

5.2 DEVELOP THE BCM ASSURANCE REVIEW ACTIVITY SCOPE

The detail contained in the scoping document will depend on the size and complexity of the review activity to be undertaken. However, the development of the review scope should determine the following (for an example scope refer to Appendix A):

- (a) The specific aim and objectives for the assurance review activity to be undertaken.
- (b) Selection of those parts of the BCM framework that will be subject to the review activity.
- (c) Areas of the organization and stakeholders that are in-scope and out-of-scope.
- (d) Methodologies that will be used to assess, evaluate, measure or validate the BCM framework.

- (e) Specific resources that will be allocated to identified parts of the review process.
- (f) Requirements for approval of the scope.

The development of the scope may be facilitated by seeking input from key internal stakeholders (for example board and management committees, process owners) and external stakeholders (such as key customers, insurers, regulatory agencies, industry bodies). This input should be further supplemented by information from available related literature (e.g. audit reports, research articles, whitepapers, regulations).

The scope should be reviewed and approved by an appropriate authority, such as the project sponsor or senior management of the organization.

5.3 ESTABLISH AIM AND OBJECTIVES

The aim and objectives of the review activity will provide the basis for the drafting of the scope and for the subsequent development and conduct of the review process. The objectives of assurance review activity should define how the aim will be achieved. Use of descriptors such as 'assess, evaluate, measure and validate' are used to define the review objectives.

The aim and objectives are a key input into developing the scoping document. An example aim and objectives is provided in the illustrative scope at Appendix A.

5.4 SELECT BCM AREAS TO BE REVIEWED

The scope should identify what aspects of the organization's approach to BCM will be examined in the specific assurance review activity. For example an individual review activity could encompass the entire BCM framework or only limited parts, such as (see Appendix F)—

- (a) end-to-end BCM processes in different locations or for different critical business functions;
- (b) conduct of the BIA;
- (c) documentation generated from the BCMS;
- (d) implementation of the communications strategy;
- (e) conduct of exercises and tests;
- (f) table top examination of sample of business continuity plans; or
- (g) management's demonstrated understanding of BCM arrangements.

5.5 DETERMINE METHODOLOGIES

The detailed methodology for undertaking the review should be determined, based on the following:

- (a) The review criteria, for example—
 - (i) audit against AS/NZS 5050.1 or AS/NZS 5050.2;
 - (ii) audit against the organization's documented BCM framework;
 - (iii) audit against another standard or robust third party methodology; or
 - (iv) identified legislative or contractual requirements.
- (b) The review process to be adopted, for example: field work based upon interviews, document discovery, testing regimes, template questionnaires.

5.6 ALLOCATE RESOURCES

Resources should be allocated according to specific requirements of the scope and the availability of budget. Each resource to be used in the review should be identified, such as reviewers, subject matter experts, computing, specialised equipment and administrative support.

5.7 APPROVE THE SCOPE

The draft scope should be approved by an appropriate authority before finalization. Depending on the governance requirements (developed in Clause 3.3) this could be undertaken by the project sponsor, senior management, management of the area under review, the manager responsible for the BCM program, or an external third party (for example a regulator or contractual entity). A copy of the approved signed scope should be retained for future governance purposes.

5.8 DEVELOP THE ASSURANCE REVIEW ACTIVITY PLAN

A separate plan should be developed for each BCM assurance review activity. The plan should specify the following:

- (a) The sponsor of the review activity.
- (b) The detailed methodology to be employed.
- (c) The components of the BCM framework that will be examined.
- (d) What types of information will be required.
- (e) How this information will be obtained, including—
 - (i) types of evidence that will be sought;
 - (ii) how testing will be conducted including the sampling regime;
 - (iii) individuals within the organization that will be interviewed during the field work; and
 - (iv) questions that will be posed.
- (f) Dates for commencement and completion of each activity.
- (g) The deployment schedule and activities of the allocated resources. and
- (h) The manner in which the compliance directions for the review are promulgated to managers and staff.

5.9 IMPLEMENT AND CONDUCT THE REVIEW

The review activity should be implemented as detailed in the plan and conducted as a robust process that includes the following steps:

- 1 Appointment of review team members.
- 2 Notification of commencement of fieldwork to management of the areas to be reviewed.
- 3 Directions and requests for access to documentation (including provision of a signed authority to access and remove documents if required).
- 4 Commencement and completion of field work.
- 5 Fieldwork close out meeting with management of areas reviewed.
- 6 Drafting of audit conclusions and recommendations, focusing on—
 - (i) addressing both causes and consequences;

- (ii) identifying corrective actions;
 - (iii) identifying preventive action; and
 - (iv) determining strengths and good practices that should be continued or reinforced.
- 7 Draft report review meeting with management.
- 8 Collation of management responses to recommendations.
- 9 Report finalization and release.

Examples of BCM assurance review activity process templates are provided at Appendices B, C, D and E.

5.10 SUITABILITY OF PROVIDERS

The selection of suitable auditors and/or reviewers is critical to ensure the success of the review, as well as the ongoing success of the business continuity management program. Selection criteria should consider the following:

- (a) Relevant knowledge, skills, experience and qualifications of the nominated individual(s) and selected third party firms (where appropriate) of—
 - (i) the organization's industry sector,
 - (ii) specific issues being reviewed (e.g. network restoration); and
 - (iii) type of review activity being considered (for example a compliance audit).
- (b) Demonstrated knowledge and understanding of the relevant legislation/ regulations for the industry sector.

5.11 REPORTING

At the completion of the assurance review, the reviewer should provide an initial verbal briefing of the findings, observations and recommendations that will be included in the overall written report.

A draft written report should be prepared that provides—

- (a) a clear understanding of the scope, including aims and objectives, of the review;
- (b) a list of the relevant legislation, standards and guidelines that are applicable;
- (c) an identification of the key risks identified and the effectiveness of the controls in their management;
- (d) a detailed description of findings and observations;
- (e) if applicable, a comment as to the extent to which the organization has or has not meet the aim and objectives of review; and
- (f) a list of recommendations in priority order;

The managers of the area under review and the project sponsor should be offered the opportunity to discuss the findings with the review team prior to responding to the recommendations. The report should be finalized on receipt of management's responses to the recommendations made in the draft report. Copies of the report should be provided to the appropriate authorities as defined in the governance requirements.

Follow up to any corrections, risk treatments and other managements actions that have been agreed to should be undertaken as part of the BCM assurance program processes.

APPENDIX A
EXAMPLE BCM ASSURANCE REVIEW ACTIVITY SCOPE
(HYPOTHETICAL ONLY)

(Informative)

ACME PTY LTD	
BCM review scope	
Aim and objectives	To provide assurance to the Board regarding the efficacy of the BCM program, through— <ul style="list-style-type: none">• A review of the compliance of the processes and procedures in place with the documented and agreed BCM framework• Benchmarking the current program against nominated industry practices
Areas for review	<ul style="list-style-type: none">• Central management of the BCM program• Areas of the organization with responsibility for designated critical business functions
Methodology	<ul style="list-style-type: none">• Interviews with responsible managers• Review of documented policies, processes and procedures against approved standards• Testing of implementation of program for each critical business function• Sample testing of representative business continuity plans
Resources	Di Larfing, Lead Auditor Con Plian, BC auditor Sil Chip, IT auditor
Timelines	Field work: commence 1 June, complete 30 June Draft report: 15 July Report finalized: 15 August Report to 30 August Audit Committee meeting
Project sponsor	Rob Hust, Executive Director Group Resilience

APPENDIX B
 EXAMPLE BCM ASSURANCE APPROACH
 (Informative)

Review concern	Review consideration—examples
Aims and objectives	<ul style="list-style-type: none"> • Aims and objectives are developed, agreed and documented • Aims and objectives provide direction for subsequent activities
Policy	<ul style="list-style-type: none"> • The policy is clearly articulated and documented. The policy provides the intent and requirements for the organization
Scope	<ul style="list-style-type: none"> • Scope is agreed and documented • Scope identifies areas inclusions and exclusions • Scope meets organization’s requirements
Planning	<ul style="list-style-type: none"> • Documented plans are developed reflecting the requirements of the aims, objectives and scope, and provide the means by which the policy will be implemented
Roles and responsibilities	<ul style="list-style-type: none"> • Roles and responsibilities are agreed and documented • Roles and responsibilities provide appropriate governance, management and technical coverage
Authority	<ul style="list-style-type: none"> • Clear accountabilities for decisions, approvals, etc, are documented • Delegations of authorities are appropriate, approved and monitored
Communication and consultation	<ul style="list-style-type: none"> • Development of the framework is undertaken with appropriate communication and consultation
Program development	<ul style="list-style-type: none"> • Robust program has been developed consistent with aims, objectives and scope
Processes	<ul style="list-style-type: none"> • Processes are conducted according to documented procedures
Resourcing	<ul style="list-style-type: none"> • Resource requirements for the program have been identified and documented • Resource allocation is adequate to achieve the aims and objectives
Monitoring and review	<ul style="list-style-type: none"> • Each part of the system, framework and processes and monitored and reviewed on according to an agreed schedule and on an <i>ad hoc</i> basis according to organizational need

APPENDIX C
 EXAMPLE TEMPLATE FOR REVIEW OF THE BCM SYSTEM
 (ILLUSTRATIVE EXAMPLE ONLY)

(Informative)

Review issue	Evidence and considerations
1.0 Policy	<ul style="list-style-type: none"> • Interviews with senior management to confirm their understanding, approach, involvement and commitment to BCM • Determine senior management’s role in establishing, implementing, and monitoring the BCM policy • Document evidence of effective dissemination of the BCM policy • Interviews with other staff to confirm their awareness and understanding of the BCM policy
2.0 Planning	<p>Interviews with senior management and other managers and staff and documentary evidence to demonstrate—</p> <ul style="list-style-type: none"> • understanding of the need for undertaking BCM within the organization • rigour of the approach to planning • appropriateness of competencies were deployed to conduct the planning • level of involvement of stakeholders in appropriate consultation • the establishment of milestones and other performance indicators • identification and access to required resources • communication of the finalized plan
2.1 Establishing understanding and the framework	
2.2 Establishing the awareness, understanding and commitment	<p>Interviews with senior management, other managers, staff and other key stakeholders, and documentary evidence to demonstrate—</p> <ul style="list-style-type: none"> • understanding of the structure and operation of the BCM system • understanding of the benefits that are expected to be derived from the BCM system • existence of appropriate authorities, accountabilities, roles and responsibilities • other resource implication of operating the BCM system
2.3 Establishing the context	<p>Interviews and documentary evidence that demonstrates—</p> <ul style="list-style-type: none"> • the level of establishment of the context for the BCM System • the extent to which the context is used to inform and direct subsequent activities

Review issue	Evidence and considerations
2.4 Designing and developing a framework	Interviews and documentary evidence that— <ul style="list-style-type: none"> • a BCM System framework has been developed and deployed • the extent to which the framework considers: <ul style="list-style-type: none"> • scope • policy • business case • development and implementation plans • capability development and improvement • governance and reporting • communications • incident response management.
2.5 Risk assessment	Interviews and documentary evidence— <ul style="list-style-type: none"> • that a rigorous risk assessment process has been developed and is deployed • how the risk assessment guides the conduct of the BIA • how findings from the risk assessment are reported and used to guide risk treatments
2.6 Business impact analysis	Interviews and documentary evidence— <ul style="list-style-type: none"> • how the BIA examines the impact of risks on critical business functions • that resource capabilities are considered • how workarounds are identified and their effectiveness is assessed
3.0 Implementation and operation—developing capabilities	
3.1 Developing and analysing disruption management strategies	Interviews and documentary evidence that— <ul style="list-style-type: none"> • consideration is given to the development of options for managing the impacts of disruptive risks to the organization • a range of options are considered for preparedness, stabilisation, continuity and recovery strategies • options are subjected to a cost benefit analysis as part of their analysis • identified assumptions are analysed and tested
3.2 Establishing resources and interdependencies	Interviews and documentary evidence— <ul style="list-style-type: none"> • that resource requirements are identified • how resource are obtained or planned for • a sufficient range of resources are considered
3.3 Developing disruption communications	Interviews and documentary evidence of how communications requirements are identified, planned for and managed
3.4 Developing documented plans	Interviews and documentary evidence— <ul style="list-style-type: none"> • of a robust process for the development of plans • that a plan(s) has been developed that considers preparedness, stabilisation, continuity and recovery requirements.

Review issue	Evidence and considerations
3.5 Documentation and its control	<p>Interviews and documentary evidence that a process or system is place for the control of all documentation related to the BCM system, and that it considers—</p> <ul style="list-style-type: none"> • preparation • version control • dissemination • storage • retrieval • protection • review • disposal
3.6 Activation and deployment	<p>Interviews and documentary evidence of—</p> <ul style="list-style-type: none"> • how plans will be activated and managed during and following an incident • a process for developing and implementing incident management plans
4.0 Performance assessment	
4.1 Monitoring and review	<p>Interviews and documentary evidence of processes in place for monitoring and reviewing the framework and each component of the BCM system, and the frequency with which such monitoring is undertaken</p>
5.0 Improvement	
5.1 Establishing maintenance processes	<p>Interviews and documentary evidence of how monitoring and review is used to ensure ongoing maintenance of the BCM system; including—</p> <ul style="list-style-type: none"> • processes that are employed • maintenance schedules that have been developed • mechanisms for initiating ad hoc reviews and improvements
5.2 Maintaining understanding	<p>Interviews and documentary evidence of how understanding of the BCM system of internal and external stakeholders is maintained</p>
5.3 Maintaining performance	<p>Interviews and documentary evidence of how the organization maintains the performance of the BCM system through preventive and corrective actions, and other continuous improvement activities</p>
5.4 Exercising	<p>Interviews and documentary evidence of a robust process for the design, development and conduct of exercises and tests of the plans and capabilities of the organization</p>
5.5 Management review	<p>Interviews and documentary evidence of how management reviews are conducted and how these are used to ensure the ongoing appropriateness and performance of the BCM system</p>

APPENDIX D

EXAMPLE TEMPLATE FOR A REVIEW OF THE BCM PROGRAM
(ILLUSTRATIVE EXAMPLE ONLY)

(Informative)

Review issue	Evidence and considerations
1.0 The business continuity management policy	
1.1 A business continuity policy has been developed and documented	<ul style="list-style-type: none"> • Evidence that a documented policy exists and is being followed • The currency of the document can be determined, eg by drafting date, version number, etc • A review date for the document is identified
1.2 The policy identifies the need, scope and objectives and accountabilities for business continuity	<ul style="list-style-type: none"> • The policy identifies the areas of the business for which business continuity is required • Objectives for business continuity are clearly identified • Criteria are present on which to evaluate business functions for inclusion into the business continuity program • The policy covers the requirements of the key objectives and deliverable of the business • The management and conduct of the business continuity program is documented • Clear roles and responsibilities are assigned to named individuals for the conduct of the business continuity program • Formal accountabilities and authorities are assigned for the business continuity program (including any needs for formal authorizations, etc)
1.3 The policy establishes the requirements for monitoring, testing and reporting for business continuity activities.	<ul style="list-style-type: none"> • The policy describes minimum requirements for a regular monitoring and testing program of the business continuity program and plans. • The policy identifies named individuals or job functions for whom reports are required for— <ul style="list-style-type: none"> • monitoring of plan status and maintenance • results of testing and exercising of plans • review, updating and improvement of plans
2.0 Business continuity program governance and structure	
2.1 Senior management understand the need for and support the business continuity management program.	<ul style="list-style-type: none"> • Documentation evidencing that senior management have been briefed on the program and have given their approval and support • Evidence of involvement of senior management as champions of the business continuity program • Evidence of senior management allocating specific resources (people, time budget etc) to the achievement of business continuity objectives

Review issue	Evidence and considerations
2.2 A plan has been developed for the BCM Program.	<ul style="list-style-type: none"> • Documented plan for the conduct of business continuity activities over a defined period of time • Defined scope or range of business continuity activities to be conducted • Establishment of documented timelines, milestones, outputs etc
2.3 Scope of required BCM activities are identified	<ul style="list-style-type: none"> • The policy, business continuity plans or other documents (identified) specifically identify those areas or critical business functions of the organization that require BCPs to be developed • Those critical business functions identified provide a sufficient comprehensive coverage to ensure continued achievement of critical business objectives in the event of a disruption
3.0 The risk analysis	
3.1 A risk analysis using a robust assessment tool has been conducted considering both internal and external contexts.	<ul style="list-style-type: none"> • A robust tool is used (e.g. ISO 31000— 2009) • Users of the tool have good familiarity with its use (may involve using expertise from elsewhere in the business or externally for example) • A broad range of threats and risks with potential disruption impacts are considered
3.2 Appropriate outputs have been developed that inform subsequent steps of the assessment and the development of capabilities	<ul style="list-style-type: none"> • The risk analysis provides a prioritized list of risks that can be used to inform the subsequent evaluation undertaken as part of the BIA • The analysis provides an indication of areas of vulnerability to disruption risk
4.0 The business impact analysis	
4.1 Appropriate managers, staff and other stakeholders have provided data and information.	<ul style="list-style-type: none"> • Critical business function and process owners/operators have been consulted and/or provided input into the BIA • In particular data/information on interdependencies both within and external to the organization have been included
4.2 All relevant critical business functions have been included.	<ul style="list-style-type: none"> • The BIA has included an assessment and prioritization of business functions critical to business success • Business areas providing essential support to the critical business functions have been included
4.3 Consideration of key risks/disruption scenarios is included	<ul style="list-style-type: none"> • Outputs from the risk analysis (as described in '3.0' above) are used to guide the conduct of the BIA

Review issue	Evidence and considerations
<p>4.4 The business impact assessment identifies all necessary key information requirements</p>	<p>The BIA considers—</p> <ul style="list-style-type: none"> • impacts of identified disruption scenarios on critical business function capability (eg rated consequences, potential disruption periods etc) • IT system dependencies and maximum acceptable outage times (or equivalents) • critical function/process success factors, including any time-related performance requirements, • key resources • post disruption recovery objectives are identification and documentation • key functional interdependencies
<p>5.0 Testing and Exercising plans</p>	
<p>5.1 There is a regular cycle of plan testing, review and improvement in place.</p>	<p>Evidence may include—</p> <ul style="list-style-type: none"> • documented test plans and protocols • conduct of exercises, with attendance by appropriate managers and staff • conduct of audit and assurance programs • findings from test exercises are incorporated into a process for improving the quality and use of continuity and recovery plans • currency of plans, e.g. the conduct of a regular 12 monthly review and update cycle
<p>5.2 Unscheduled plan revision</p>	<ul style="list-style-type: none"> • Processes are in place to allow for unscheduled revision of business continuity plans, eg following major structural reorganizations, departure of key staff etc • A post incident review process (e.g. debriefing) has been established
<p>5.3 Awareness and training of BCP is conducted</p>	<p>Evidence of this could include—</p> <ul style="list-style-type: none"> • existence of documented training packages • conduct of training courses for individuals with business continuity plan responsibilities • managers and staff with ownership of critical business functions are exposed to the content of the BCPs
<p>6.0 Communications</p>	
<p>6.1 Communications objectives and strategies for the BCM program, have been developed</p>	<p>Documented objectives and strategies identifying—</p> <ul style="list-style-type: none"> • who • what • where • when • why • how
<p>6.2 Strategies and plans have been implemented and monitored.</p>	<ul style="list-style-type: none"> • Relevant areas of the business have received appropriate communications, have participated in program development activities etc.

APPENDIX E

EXAMPLE TEMPLATE FOR A REVIEW OF BUSINESS CONTINUITY PLAN
(ILLUSTRATIVE ONLY)

(Informative)

Review issue	Evidence and considerations
1.0 Governance of BCPs	
1.1 The finalized plan has been returned for review	Finalized plans have been signed off by the business areas and have been reviewed at a corporate level
1.2 Scope of required plan activities are identified	The BCP specifically identifies the— <ul style="list-style-type: none"> • Business area responsible for the BCP • The Critical Business Functions and processes covered by the BCP • The location of the function • Those critical business functions identified provide a sufficient comprehensive coverage to ensure continued achievement of critical business objectives in the event of a disruption
1.3 BCP coverage	The collected BCPs for a given area or activity of the business provide appropriate and adequate coverage of the relevant critical business functions. Requirements for the successful achievement of business objectives and to meet contractual conditions are covered by the range of BCPs developed
2.0 Functional details	
2.1 Responsible officer	A responsible officer(s) for the plan has been identified
2.2 Key process and sub processes	The key processes and sub-processes required for the successful delivery of the critical business function have been identified
2.3 Critical success factors	Critical success factors have been identified and have been qualified with measurable parameters for each critical business function
	The critical success factors provide guidance on service delivery levels requirements and/or likely stakeholder expectations that have to be managed during a disruption
2.4 Functional interdependencies	Internal and external interdependencies with the critical business function are clearly identified
2.5 Staff Contact details	Contact details are provided for each key staff member, including— <ul style="list-style-type: none"> • Role and responsibilities • BH telephone • Mobile or AH number • Email address • Identified deputy or stand-in

Review issue	Evidence and considerations
3.0 Workload and time dependencies	
3.1 Workload and time dependencies	Seasonal and weekly workload demands have been mapped
3.2 Maximum acceptable outage times	Maximum acceptable outage times and minimum acceptable levels of performance for the function are identified
3.3 Scenario impacts	Time based impacts for each of the scenarios are identified
3.4 Resourcing requirements	Resourcing requirements under normal and disrupted operations are identified for— <ul style="list-style-type: none"> • IT applications • Office equipment • Documentation • Staff • Services and equipment • Facilities
3.5 IT dependencies	Maximum acceptable outage times are recorded for each of the dependent IT systems and applications
4.0 Continuity arrangements	
4.1 Continuity processes and workarounds have been developed	This could include, for key disruption scenarios— <ul style="list-style-type: none"> • Identification of what processes can still proceed under the disruption scenario • Identification of what processes will be affected by the disruption scenario • Where applicable identification of alternate (e.g. manual) workarounds that can be implemented • Where required, arrangements for the processing of work backlogs • Identification of those processes likely to be unaffected by the disruption
4.2 Process responsibilities identified	Documentation of identified personnel responsible for individual key functions processes, activities etc Deputies/alternates are identified for key roles
4.3 Continuity mgt activities	Specific continuity management activities are identified for key personnel, for example steps to be taken up to and from the activation of the business continuity plan
4.4 Client and stakeholder	Where critical stakeholders exist, provision of— <ul style="list-style-type: none"> • contact details • service expectations • alternate arrangements
4.5 Suppliers	Where critical suppliers exist, provision of— <ul style="list-style-type: none"> • contact details • service expectations • alternate arrangements
4.6 Communication plans	Communications requirements during a disruption are identified including— <ul style="list-style-type: none"> • message details, who, how, what, where, when • authorizations

APPENDIX F

EXAMPLE OF REVIEW AREA WITHIN THE BCM FRAMEWORK
(ILLUSTRATIVE EXAMPLE ONLY)

(Informative)

An assurance activity could be conducted over the whole of the BCM framework, or may focus on only selected areas or elements. Figure F1 illustrates some areas of the BCM framework that could be selected for assurance review activity.

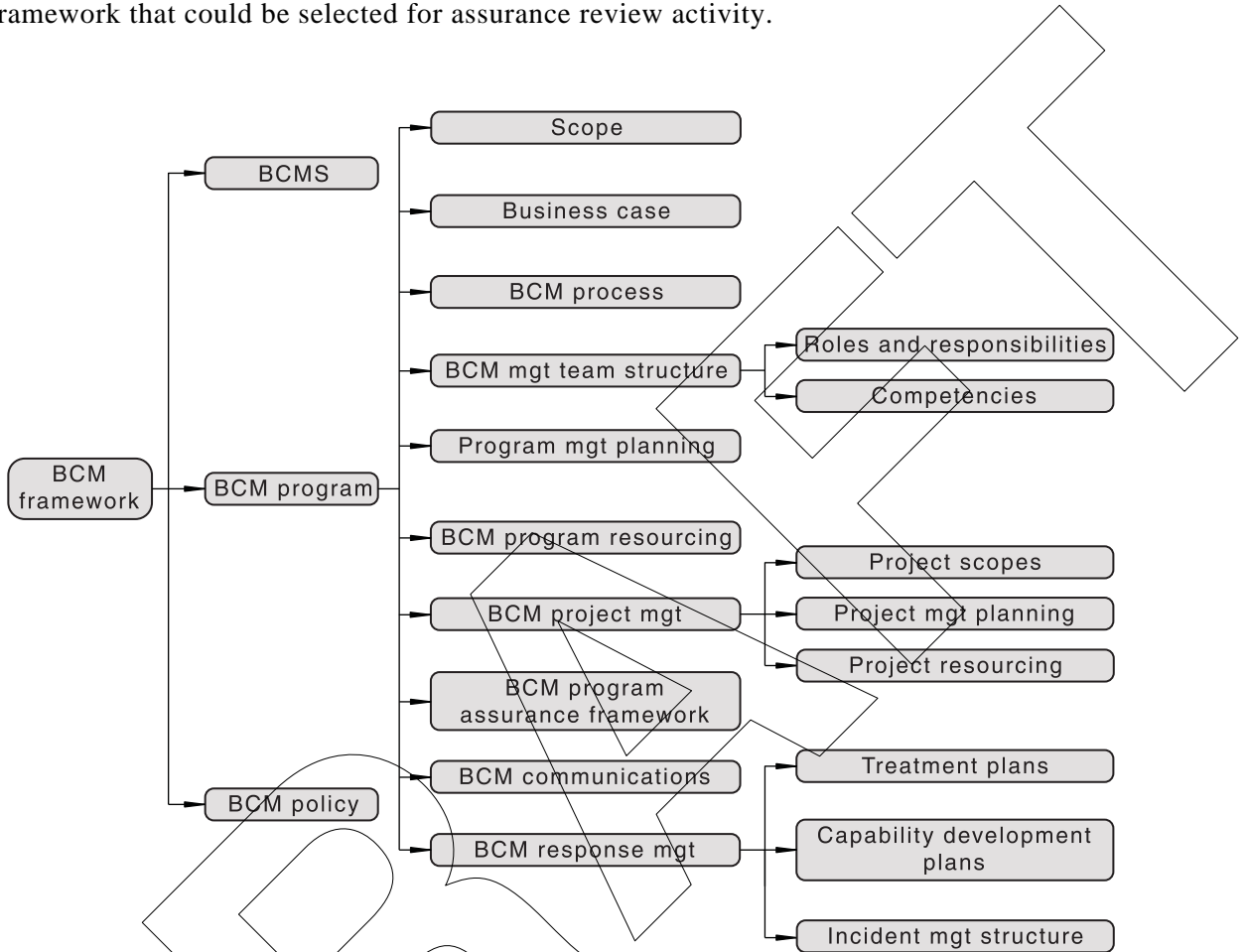


FIGURE F1 ILLUSTRATIVE EXAMPLE OF THE ELEMENTS OF A BCM FRAMEWORK

*** 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.com.au

www.standards.co.nz