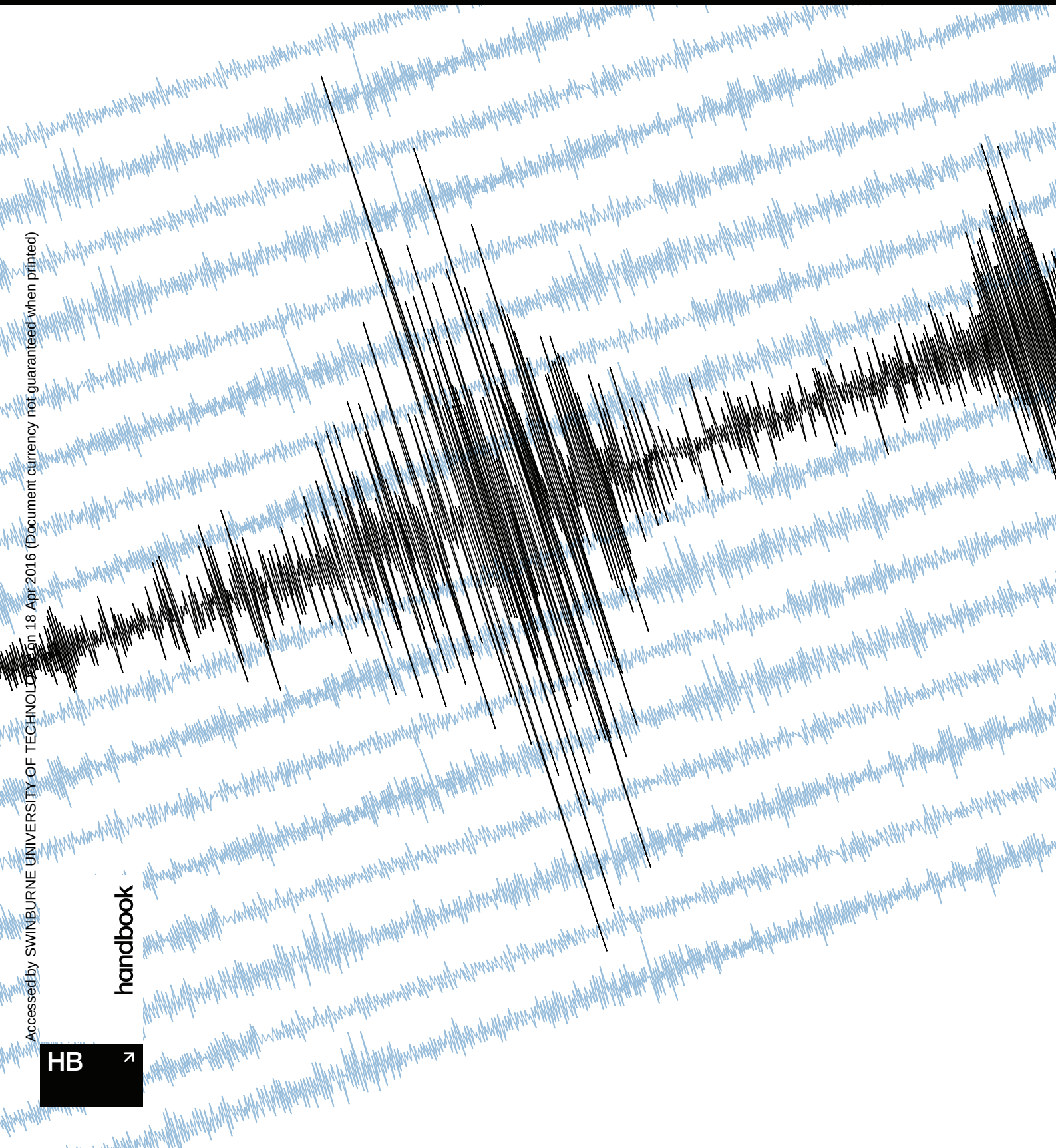
STANDARDS Australia

HB 292—2006

A Practitioners Guide to Business Continuity Management



handbook

HB

Handbook

A practitioners guide to business continuity management

First published as HB 292—2006.

Published by Standards Australia, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 7472 5

Preface

This Guide provides an overview of selected 'generally accepted practices' and emerging new practices used variously within Australasia, USA and UK. Business Continuity Management (BCM) practice is such that approaches that work well in one organisation may be wholly inappropriate for a different organisation. Extreme care therefore needs to be taken in deciding what and how aspects of BCM will be implemented within an organisation.

The structure of the Guide is based on Standards Australia/ Standards New Zealand Business Continuity Management Handbook HB 221:2004. Much of the information presented is fully consistent with HB 221. However, the principles of HB 221 have been significantly expanded upon and extensive new explanatory information is provided. This material is broadly consistent with the principles of other generally accepted practices such as NFPA1600 and the BCI Good Practice Guidelines 2005, Spring TR19: 2005; and the work of the DRII and DRJ.

Readers need to be aware that the content of this Guide represents in-progress research by the authors and is subject to change without notice.

This Guide is not intended to provide authoritative advice and no guarantee or warranty is provided as to the accuracy or applicability of any information provided in this Guide.

Dr Carl A. Gibson and Gavin Love

January 2006

Contents

Page

1 Business continuity management?

1.1 What comprises business continuity management?

A wide range of terminology has been used to describe the processes associated with managing disruptions. Some of these terms include:

- Business continuity planning;
- Continuity planning;
- Contingency planning;
- Crisis management;
- Disaster recovery planning;
- Emergency management;
- Incident management;
- Disruption management;
- Business resumption planning; and
- Business resilience.

Originally these terms each had distinct meanings, but with time they have become interchangeable for many organisations and practitioners. This has often caused confusion and at times heated debate amongst practitioners.

In recent years the term '***business continuity management'*** (BCM) has emerged to replace this disparate terminology. Today, under the BCM umbrella, some of the terminology is beginning to return to its original meanings where:

- Business continuity planning is often used to refer to those BCM activities associated with activities that assist in the continuing availability and capability of property, people and information; and
- Disaster recovery planning is often used to refer to those BCM activities associated with the continuing availability and restoration of the IT infrastructure (but should not be confused with the wider recovery and restoration activities).

1.2 Defining BCM

The Joint Standards Australia/Standards New Zealand handbook for Business Continuity Management (HB 221: 2004) defines business continuity as:

'Business Continuity Management provides the availability of processes and resources in order to ensure the continued achievement of critical objectives.'

This is an important definition as it identifies both what a well founded approach to BCM must achieve as well as the means of achieving it:

- **'critical objectives'**

  what the organisation, project, team, individual must absolutely strive to achieve, i.e. what are the priorities and what are less important. These will ultimately direct our focus for BCM;

- **'processes and resources'**

  the processes that will allow critical objectives to be achieved, and the resources required to support those processes;

- **'availability'**

  processes and resources must be capable and accessible; and

- **'continued'**

  the capability to achieve critical objectives needs to be sustainable in the face of future uncertainty.

1.2.1 The elements of good practice

BCM is **NOT** about having a nice printed document that contains some 'what ifs' and possible responses that can be presented to senior management, the Board or auditors to earn a tick off and then be stored in a drawer. BCM **IS** about having a robust process that allows individuals to:

- Better understand uncertainty about the future;
- Realise the potential for different types of disruption;
- Better plan for future management of those disruptions, and to put in place business improvement *now* to reduce the likelihood and/or consequence of significant future disruption.

The interrelationship of these elements is summarised in Figure 1.

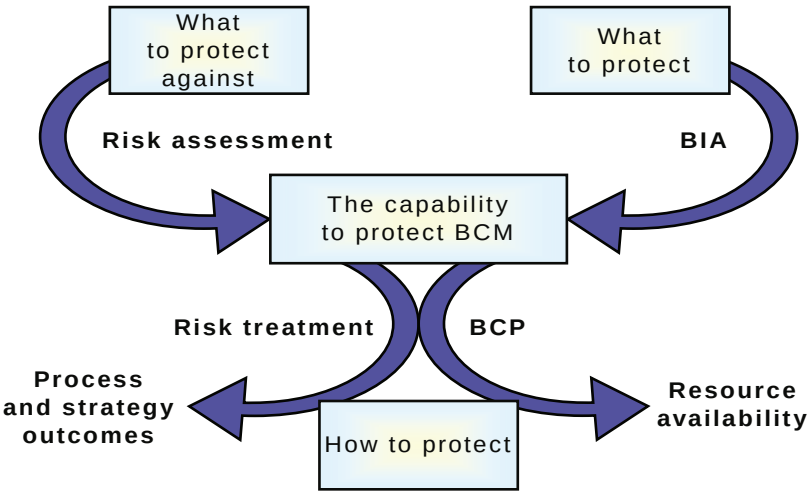


FIGURE 1 KEY FUNCTIPNAL ELEMENTS OF BCM

Put simply, the BCM framework illustrated in Figure 1 should help us to answer the following questions:

- What could happen?
- So what does it mean to me?
- What is critical to continuing our business?
- What do we have to do before, during and after an incident/event/crisis/emergency?

1.3 The nature of crises and disasters

In recent years much of the business continuity literature, particularly in the less specialised publications, has concentrated on managing the impacts of organisational crises following spectacular incidents. Such dramatic crises are usually perceived as having originated from events such as natural disasters, catastrophic loss of utility, large industrial accidents or collateral damage following acts of violence. However, research conducted by the Institute of Crisis Management in 2004 suggests that such crises represent less than 20% of the total reported causes of organisational crises (see Figure 2). The vast majority arise from the escalation of routine management issues to significant disruptive events.

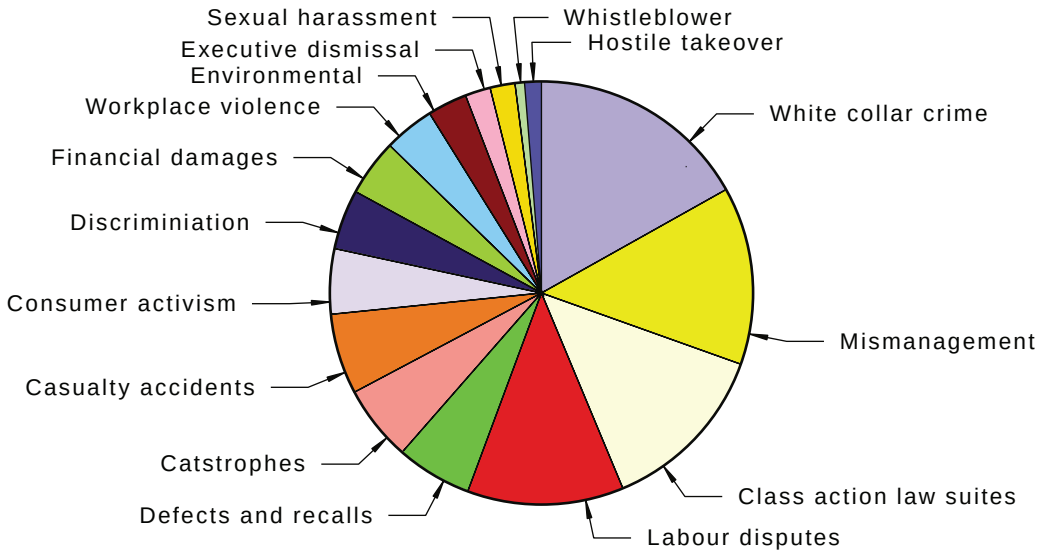


FIGURE 2 CAUSES OF ORGANISATIONAL CRISIS*

It is therefore critically important that these other more 'mundane' and 'routine' events are not ignored when considering possible causes of crises that may require a business continuity solution in their management.

1.3.1 Crisis versus disaster

In many organisations 'crisis' and 'disaster' are used interchangeably. However, in practical terms the two are different both in terms of escalation of event and its treatment. One of the prime purposes of management in an organisation is to make decisions regarding an uncertain future (i.e. manage the strategic and operational risk). Occasionally, these decisions (or lack of decision) will result in an untoward event occurring that potentially or actually results in a disruption to the day-to-day operations of part or the whole of the organisation. Such an event is defined as a ***crisis***, where management is required to divert a proportion of their attention, time, energy and resources away from normal operations to managing this untoward event. If the crisis escalates further and overwhelms management's capabilities to cope, control will begin to be lost and the event will then be regarded as a ***disaster***.

Crises do occur on a regular basis and are usually characterised by being managed by existing internal resources. Conversely, disasters are usually characterised by individuals or groups taking on significant new roles and responsibilities, often with external agencies taking over management of the event (Figure 3).

---

* Source of data: ICM Report 2004.

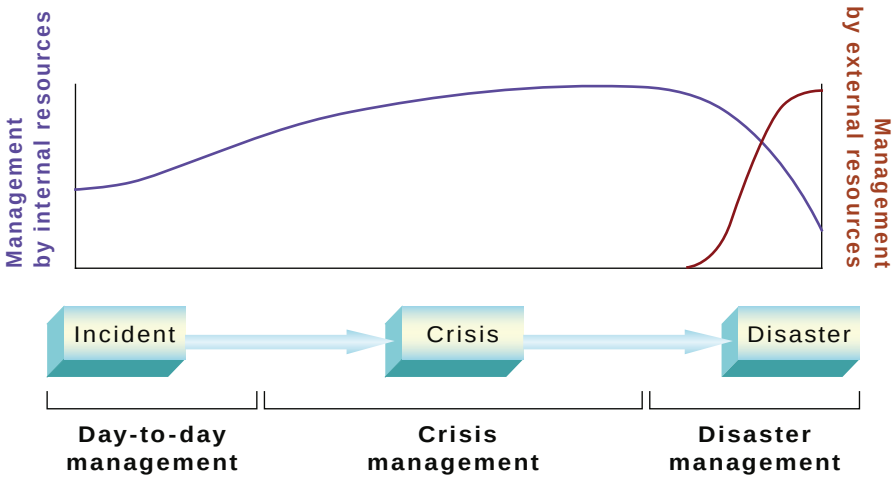


FIGURE 3 MANAGEMENT OF A CRISIS VERSUS A DISASTER

1.4 Different approaches to business continuity and common elements

As yet there is no internationally defined or accepted standard for business continuity. Within Australia there is a joint Standards Australia and Standards New Zealand publication: *Business Continuity Management* HB 221:2004. This publication is based on generally accepted practice principles from within Australasia and internationally. Another excellent publication, although a little dated, is the Australian National Audit Office – *Keeping the Wheels in Motion*. The Australian Prudential Regulatory Authority has also published a draft standard* that provides useful summary of the key elements of BCM. In the UK, the British Standards Institute has released the *PAS*† *56 BCM Guide to Business Continuity* based upon the *BCI's Good Practice Guidelines*, whilst in the USA there is the NFPA‡1600 standard and the Disaster Recovery Institute International's (DRII) *Ten Professional Practices* and more recently the *Generally Accepted Practices for Business Continuity Practitioners*§. In essence these methodologies each demonstrate a similar approach, there are only slight differences in terminology and the structure of the flowchart in which the key elements are aligned (Figure 4). The major difference is that the Australian and USA approaches recognise the fundamental interrelationship between risk management and business continuity management, whilst the British approach views the relationship more distantly.

---

* Prudential Standard XPS XXX, APRA, July 2004.

† PAS= publicly available specification

‡ NFPA= National Fire Protection Association

§ A joint Disaster Recovery Journal and DRII initiative

This Guide is closely aligned with the principles of AS/NZS HB 221: 2004 and is broadly consistent with other international approaches.

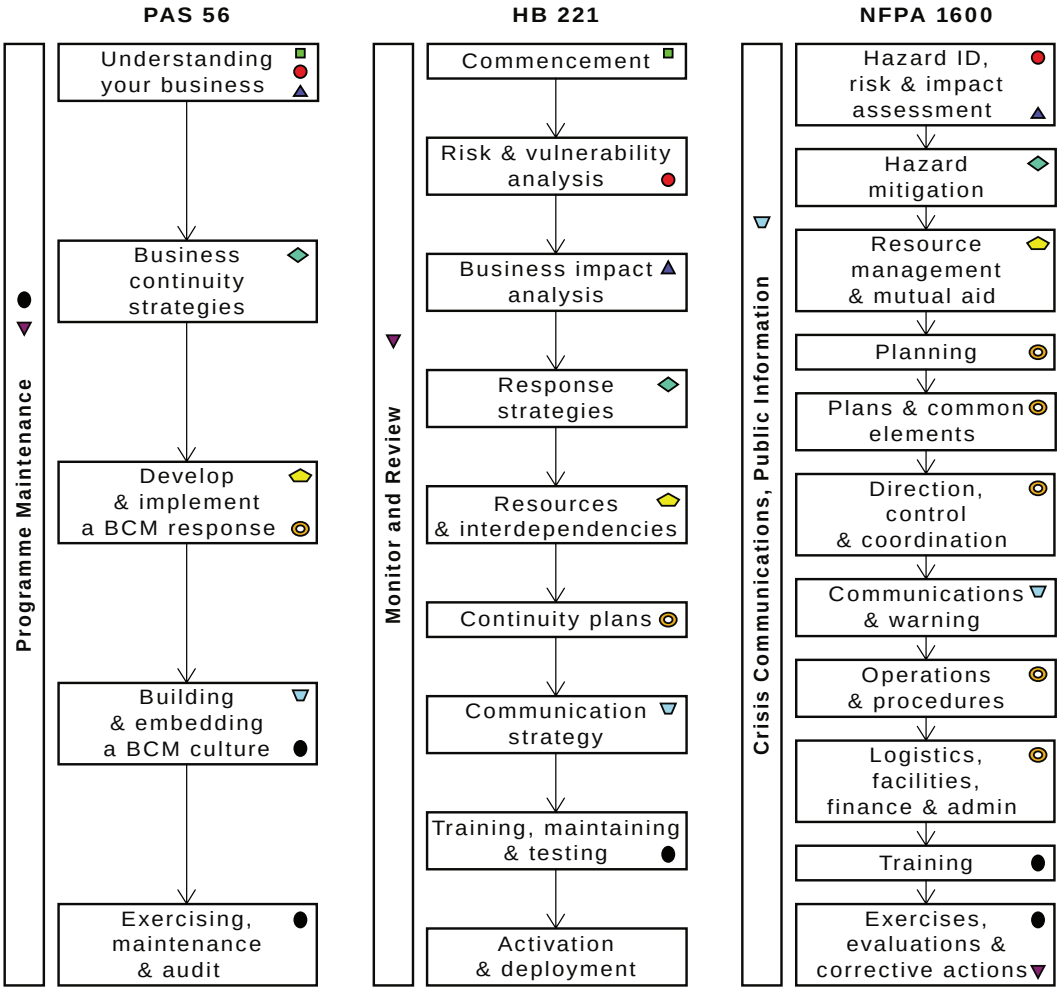


FIGURE 4 THE RELATIONSHIP BETWEEN AUSTRALIAN, BRITISH AND US APPROACHES*

* In HB 221, each stage is represented with a unique symbol. The location of the processes in PAS 56 and NFPA 1600 are denoted by the corresponding symbol.

1.5 BCM: Interrelationships with other disciplines and activities

Traditional thinking has positioned risk management as a tool to be used within business continuity; a paradigm that (with some practitioners and organisations) has long outlasted its origins in IT disaster recovery planning. More contemporary thinking sees risk management as a broad philosophy looking at understanding uncertainty, informed decision making and managing 'surprise' in the achievement of objectives. This thinking also views BCM as an integral part of the broad field of risk management, a part that considers the management, both pre- and post- event of those risks that may result in disruption to the organisation.

Confusion has entered the debate where protagonists on either side have misunderstood the basis of risk management. Such misinformed debate has often centred on 'risk management' being the function within an organisation's structure, and has argued aimlessly around which function - 'BCM' or 'risk management' should be subordinate to one another. This has ignored the broader perspective that risk management is focused on the better understanding of uncertainty and more informed decision making in its management.

There are numerous benefits of this more contemporary approach to risk and business continuity, over the traditional paradigm. These include:

- More holistic and comprehensive consideration of risk within the BCM process;
- Improved integration between BCM and risk management activities within the organisation, including:
  - improved flows of risk related information,
  - better understanding of requirements of both activities than when separate,
  - lessened repeated demands on the organisation for the same sets of information;
- Appropriate organisational ***focus on priority risks***, including those related to business continuity;
- More ***cost effective use of resources*** (time, people and budget); and
- Improved focus of BCM activity on ***business improvement***, rather than just reactive planning.

Today, most accepted practices in both BCM and risk management have such significant areas of commonality in approach, stakeholders and information flows that it is commonsense to capitalise on their synergies through integrating at any level.

1.6 What are the benefits of implementing BCM?

At its core BCM is about planning for the future, and as with any type of planning, (for example business, corporate, strategic, commercial, etc), *a failure in planning is planning to fail.* However, identifying and measuring the cost benefit of the investment being made in BCM is a much more difficult proposition. Some of the benefits of implementing and maintaining an effective BCM capability are summarised in Table 1.

Table 1
Example benefits arising from effective BCM

Tangible benefits	Intangible benefits
Improved protection of shareholder value.	Preservation of market base.
Compliance with regulatory requirements.	Managed exposure to risks of business disruption.
Compliance with clients' contractual requirements, and avoidance of liability and penalties.	Improved operational resilience to unforeseen events.
Compliance with insurance policy conditions.	Preservation of reputation through ensuring continuity of supply.
Reduced operational downtime.	Improved efficiency and effectiveness of processes.
Reduced costs of operating during a disruption.	Provision of real competitive advantage.
Reduced losses as a result of a disruption.	Improved staff confidence.
Reduced costs of backlog management.	Improved stakeholder confidence.
More cost effective recovery.	Improved process understanding.

1.7 The BCM process

The BCM process provides a rigorous logical planning process that will assist an organisation to respond appropriately to a wide range of disruption risks. However, there is more to undertaking business continuity than the simple writing of a business continuity plan (BCP). Plans need to reflect the changing nature of both internal and external environments, and the changing demands of the organisation and its stakeholders. The writing of a BCP therefore needs to be conducted as part of an appropriately managed BCM program.

The key steps in BCM are (see Figure 5):

- **Commencement**

  Business continuity is implemented within an organisation to focus on the sustainability of key business objectives, and on developing an understanding of, and commitment to BCM.

- **Risk and vulnerability analysis**

  Understanding of the hazards and threats facing the organisation is developed, how these factors can create risks of business disruption and the organisation's vulnerabilities to these risks are investigated.

- **Business impact assessment**

  The potential organisational effects of disruptions are determined and the resources and capabilities required to continue the business operations following these disruptions are identified.

- **Disruption strategies**

  Emergency response, continuity and recovery strategies are developed to provide effective management of priority disruption risks.

- **Resources and interdependencies**

  Resource requirements from across an organisation are consolidated and mapped according to business priorities and interdependencies internal and external to the organisation are identified and managed.

- **Plan documentation**

  The information collected and developed during the BCM process is used to create written plans that can be used practically to implement and manage the required activities following an incident.

- **Disruption communications**

  The organisation informs internal and external stakeholders on issues regarding documented plans and planned actions prior to an incident occurring. Stakeholder information needs following any activation of plans are also addressed.

- **Maintenance**

  The organisation continues to develop BCM capabilities and ensure that plans remain relevant and up-to-date.

- **Activation and deployment**

  The organisation ensures that strategies are implemented and managed appropriately.

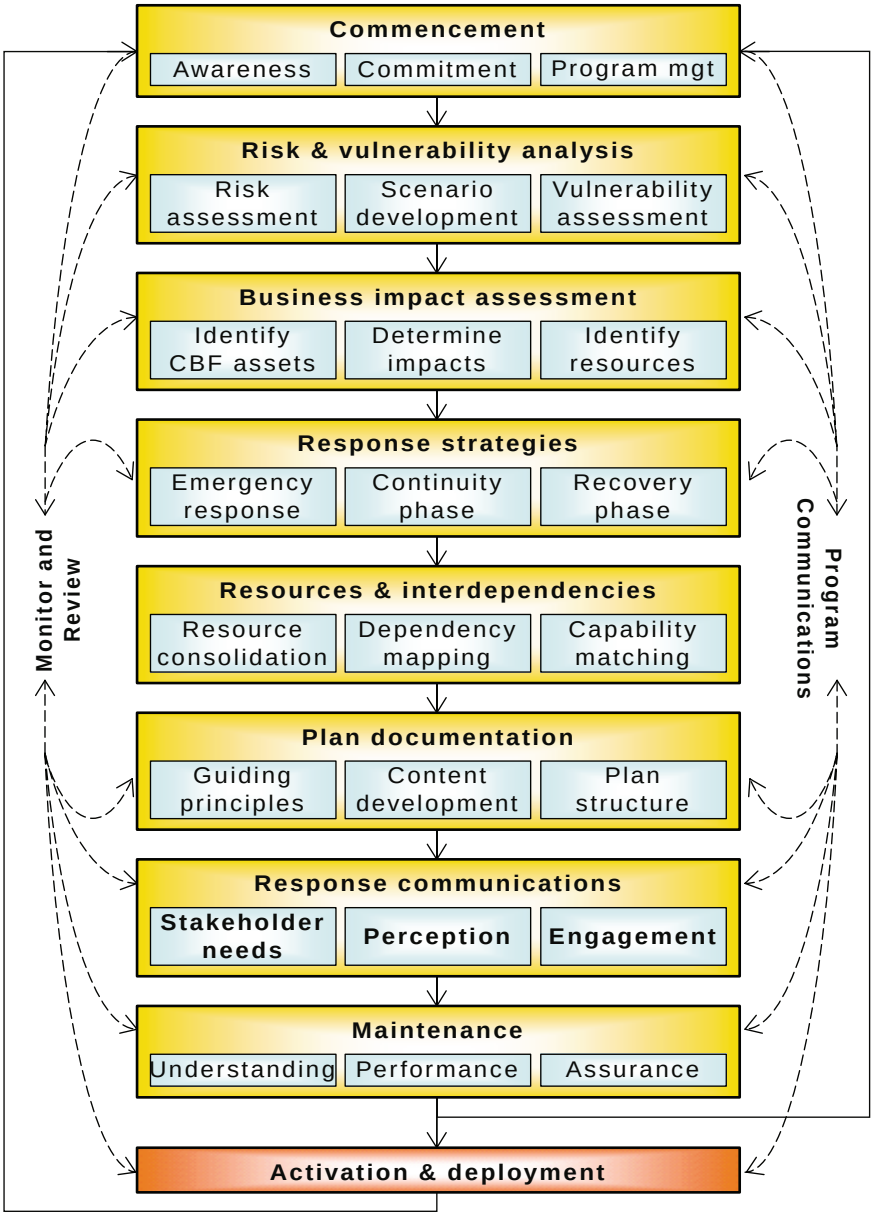


FIGURE 5 THE BCM PROCESS

1.8 Summary

- There are many causes of organisational crises, however, less than 20% of the total is attributed to traditional disasters of environmental, casualty accidents, catastrophes and workplace violence.
- BCM is a contemporary term that replaces the wide variety of terminology used traditionally.
- BCM provides for the availability of processes and resources in order to ensure the continued achievement of critical objectives.
- BCM is a logical reiterative process that has a number of features common to all acknowledged international approaches.

- BCM is a more embracing concept than just business continuity planning.
- BCM is an integral component of managing risk, with a focus on those risks that could disrupt the achievement of objectives.
- Effective BCM is concerned with:
  - understanding uncertainty,
  - understanding what's important to the organisation,
  - ensuring that critical business objectives continue to be achieved,
  - ensuring that critical processes continue to operate, and
  - ensuring that critical processes are supported.
- BCM comprises a logical reiterative process that has a number of features common to all acknowledged international approaches.

2 Commencement of Business Continuity Management: establishing a framework and managing the program

2.1 Introduction

The *Commencement* step of BCM establishes the infrastructure and much of the capability required for each of the other steps of the process. Commencement is concerned with:

- Creating ***awareness and understanding*** of BCM and the skills required;
- Gaining the ***commitment*** and support of management and staff for the implementation and ongoing maintenance of BCM; and
- Establishing the organisational infrastructure ***program management*** required for a successful implementation.

2.2 Awareness and understanding

One of the first activities to be undertaken in the commencement step is to begin to create an awareness of the potential for disruption and an understanding of what the organisation needs to do to manage it. This will require a well-founded understanding of both the organisation *and* the environment within which it is operating. In essence this is about seeking the answers to three fundamental questions:

'What is important to the success and sustainability of my organisation?'

'What does my organisation depend upon to continue operating?'

'What might prevent my organisation from achieving its key objectives?'

There may be some 'short cuts' that can be exploited to save both time and budget in seeking this information. For example, if the organisation has a corporate risk management program, much of the information for BCM's '*Awareness and Understanding*' activities can be derived from risk management's '*Context*'. Key components of determining the organisational need for BCM should include:

- Understanding the key imperatives of the organisation, including:
  - critical objectives, critical success factors and key performance indicators,
  - major current and emerging risk exposures (including identifying both threats and opportunities);
- Critical organisational dependencies and interdependencies, within and external to the organisation, including:
  - critical business functions and processes,
  - critical plant, property, assets and other infrastructure,
  - critical people and information resources,
  - third party relationships such as with the community, suppliers, customers, partners and regulators;
- Analysis of past incidents and disruptions that indicate a propensity for future disruption, including:
  - occurrences in the area of the organisation under consideration,
  - occurrences in the organisation as a whole,
  - prior involvement of key interdependencies, such as customers, suppliers, strategic alliances and other stakeholders,
  - experiences of others within the same market sector, industry, geographical location, etc; and
- Identifying and agreeing upon the scope for BCM, including issues such as:
  - the goals and objectives of strategic and operational activities of BCM,
  - expected deliverables and outcomes,
  - time requirements, demands or constraints,

- resourcing capabilities and limitations,
- geographical extent and boundaries,
- organisational structure, extent and boundaries.

2.3 Gaining management commitment

The majority of the BCM literature puts forward the position that gaining the support and commitment of senior management and the Board (where applicable) is essential to the implementation of effective BCM. It is possible to implement components of BCM in the absence of this support. However, attempting it in the absence of such commitment and support is exceptionally ***difficult***, is far more ***prone to failure*** than success, will be ***far less sustainable,*** and is likely to be far more ***wasteful*** of resources in the longer term. Time and effort spent in gaining this commitment and support is therefore fundamental to implementing and sustaining a ***successful*** BCM program because:

- BCM activities will make continuing demands on the attention and time of individuals from across the organisation. Therefore BCM will be a distraction from other core business priorities;
- BCM activities produce information that, at times, will require dedicated management time and attention to understand and make decisions on;
- Some of the outputs from BCM will be recommendations on process improvement or re-engineering. These will usually require budget allocation and approval to proceed;
- Such improvement and re-engineering activities can impact wider areas within the organisation and impose additional constraints to routine operations;
- A number of individuals will be involved in BCM activities. This will need to be accounted for and approved;
- There may be additional expertise or equipment that has to be resourced to support the development and implementation of the BCM program.

Broadly speaking there are two approaches to gaining senior management commitment and support, through:

- ***Engagement***, where personal interest and emotional buy-in are achieved; and
- Presentation of a reasoned argument, for example through a formal ***business case.*** Although a business case that does adequately engage the decision-maker will not receive appropriate consideration.

2.4 The need for communication and engagement

Effective communication and consultation are important considerations in each of the steps of the BCM process. Communication and consultation are the fundamental means of gathering input, and of checking the validity and relevance of data and information. They are also essential in improving awareness of, and commitment to the BCM activities being undertaken. Both involve a two-way dialogue with stakeholders* with the focus on sharing information, rather than a flow in a single direction. Throughout BCM, the attention of communication should be on gaining and providing information that will assist in the tasks required to implement and imbed BCM. Developing communications for use following an incident (sometimes called 'crisis communications') is dealt with separately in Chapter 8.

Effective communication is dependent, in part, upon the choice of communication channel and its appropriateness to the content of the message and to the audience (see Section 8.4 for further information). A summary of the advantages and disadvantages of different communication channels is provided at Appendix A. Establishment of effective communications requires active engagement with stakeholders. Approaches to gaining this engagement can include:

- Clearly articulating the direct and indirect benefits to management and staff of participating in BCM;
- Identifying potential 'emotional triggers' that will assist in personalising and prioritising issues for stakeholders (for example employees that have experienced disruption from flooding will be more receptive to BCM that talks about such mundane issues, compared to an approach that focuses on the catastrophic disruption of a terrorist attack);
- Recognising and managing one's own and other parties' perceptions of risk (see Chapter 8 for a further discussion on perception);
- Aligning with and building upon synergies with other activities;
- Providing an understanding of what will be expected in terms of time and resources;
- Providing an appropriate level of ownership of the BCM program to others;
- Increasing overall awareness by sharing both success stories and calamities that have been experienced by others; and
- Providing a voice for issues of concern to stakeholders.

---

* Stakeholders – Appendix I Glossary for more detail.

2.5 Preparation of the business case

Senior management will usually require some form of business case to justify new or changing investments in BCM activities (i.e. whether implementing BCM for the first time, expanding an existing program, or undertaking a specific one-off BCM project). Individual organisations may have their own unique formalised requirements for the preparation of a business case, however, most approaches will be based to varying degrees on the key elements summarised in Table 2.

Table 2
Summaries of key elements of a business case

Element	Description
Objectives and goals	• Objectives, goals, deliverables and outcomes of the proposed BCM activity. • Alignment with corporate/organisational objectives and/or priorities.
Governance	• Clear identification of the basis for any assumptions made. • Defined accountabilities and responsibilities, including: identification of the project/business owner, senior management sponsor, etc. • Ongoing monitoring and reporting requirements.
Organisational needs	• Identification of the organisation/business needs for BCM, including: historical data of incidents occurring within the organisation, community, industry location, area, etc. • Identification of disruption exposures.
BCM scope	• Structural extent and boundaries. • Geographical extent and boundaries. • Business function extent and boundaries. • Duration, time constraints and milestones.
Resourcing	• Internal staff, skills etc. • External expertise to be sourced. • Time demands on other areas of the organisation. • Equipment. • Accommodation.
Budget	• Budget breakdown, including: – salaries, oncost and consultancy fees, – software development or purchase, – report production, publishing, etc, – travel, accommodation and other incidental costs, – equipment and hardware (purchase or lease).

(continued)

Table 2 (*continued)*

Element	Description
Cost benefits analysis	• Implementation costs. • Other costs, to the organisation as a whole, including: – any constraints or barriers that the proposed activities may impose upon other parts of the organisation, – critical interdependencies including the demands that will be made on these interdependencies. • Projected returns and benefits, including: – tangible (eg financial) benefits (such as cost savings, for example through reduced revenue leakage). For projects with extended duration or payback periods consider including net present values (NPV), – intangible (non-financial) benefits (such as improved staff safety, improved quality of decision making, or reduced risk of unauthorised information disclosure).
Recommendation	• Consideration of options for BCM implementation including the identification rationale for the recommended option(s).

2.6 Gaining the commitment of others

2.6.1 Engagement and involvement of staff

Effective implementation requires engagement and involvement of those staff with specific BCM development or implementation responsibilities. This requires that attention is paid to the effectiveness of communications throughout the program, in particular the information needs of these staff. Other staff may also be affected by a disruption (even indirectly) and their communication and engagement needs will also require consideration.

2.6.2 Engagement and involvement of other stakeholders

Even before the issues of how to engage and involve other stakeholders are addressed, the following questions need to be addressed:

- Who are the important stakeholders?
- What information do they require from me?
- What information can I provide to them?
- What information do I require from them?

The type of stakeholders and the extent of their involvement in BCM will depend to a great extent upon the nature of their relationship with the organisation. The following stakeholders would usually be considered: suppliers, contractors, customers, community groups, industry groups or associations, academic institutions, regulators, and on occasion even competitors.

The involvement of such stakeholders in the early stages of a BCM program can provide a number of benefits:

- The stakeholder may have a greater awareness or understanding of some risk exposures than the organisation itself;
- Stakeholders will certainly look at risk exposures and their treatment from a different perspective to the organisation; and
- Any plans or process improvements may impact upon, or be constrained by one or more stakeholders. A successful implementation is more likely with the early involvement of stakeholders.

2.7 Establishing the infrastructure for BCM

Establishing the BCM program needs the careful consideration of a number of issues:

- Will a formal or informal structure for BCM be implemented?
- Will a dedicated manager for the BCM program be appointed?
- Does an implementation/management team, steering committee, etc need to be established?
- Is BCM expertise available within the organisation?
- Will expertise be recruited, contracted or will consultants be used?
- Will all BCM activities be undertaken centrally?
- What resources will be required?
- What level of responsibility and ownership of BCM reside at different levels of the organisation?
- How will BCM be deployed, for example mass implementation, staged (eg by structure, location or critical priority), or layered?
- What responsibilities need to be defined?
- How will accountabilities be defined?
- What are the implementation/project/program objectives, milestones, KPIs, deliverables, etc?
- What reporting structures need to be established?

It is usually appropriate at this stage to commence implementing the key elements that will comprise the BCM framework. This may require a revalidation or change to arrangements that have been detailed in any awareness program or business case that has been previously delivered. Key considerations include:

- The development and approval of a BCM policy;
- Confirmation of processes that will be used through the BCM program;
- Identification and assignment of resources required to implement the BCM program; and

- The establishment of structures and mechanisms for governance of the program.

2.8 Development of the BCM policy

A formal BCM policy can provide a useful guide as to what the *agreed* BCM priorities are, the approach being taken to implement BCM and who has responsibility for what activities within the program. A comprehensive policy should consider:

- The aims and objectives for business continuity management;
- The high level framework by which BCM will be implemented and managed;
- The requirements and responsibilities of areas of the organisation for participation in the BCM program;
- The parts of the organisation for which BCM is required (eg, for critical business functions, critical assets or plant, critical sites or locations, etc); and
- Accountabilities and responsibilities of groups, teams and roles within the organisation.

Policies should be reviewed annually to ensure their continuing relevance to organisational needs and should be approved by senior executive management, the Board or equivalent (where appropriate).

2.9 Confirmation of processes

The processes that will be used in each of the BCM steps need to be confirmed before further implementation is undertaken. A number of issues need to be considered in this confirmation, including:

- Are processes based upon appropriate generally accepted/better practices?
- Where processes deviate from these generally accepted practices, is there an understood valid reason?
- Are the chosen approaches suitable to meet organisational needs and are they capable of delivering the desired outcomes?
- Will the necessary resources and capabilities be available for these processes to operate effectively and efficiently?
- Will the processes impose any constraints or additional risks on the organisation that may be unacceptable?
- Are there any regulatory issues or constraints that will impose requirements on process use?

2.10 Resource allocation

Resources required for the implementation of the BCM program need to identified, agreed to by relevant management and assigned to their responsibilities. These resources may include:

- **Management and staff**

Management and staff are needed to undertake specific program tasks, or to develop and provide key information required in any of the steps of the process. Participation in BCM can be time consuming and be seen as a distraction from core activities for some individuals. This strengthens the need to ensure that attention is paid to communication and, in particular, engagement of people throughout the BCM program.

- **Consultants and contractors**

Consultant and contractors may be needed to provide additional expertise and/or capacity. The BCM program needs to be developed and implemented to meet the needs of the organisation, not be based on an external 'one size fits all' service package. Furthermore, management need to retain ownership and accountability for BCM; this should never be handed over to external providers.

- **Budget**

The implementation of the BCM program will have a cost. The expectations of the BCM program must be matched to available budget whilst senior management need to be aware of the cost of achieving their required levels of readiness and capability.

- **Infrastructure**

Accommodation (office space, meeting rooms, training rooms, etc), equipment (eg, office and communications equipment) and IT systems need to be identified, planned for, and be available when and where required. The means by which data and information will be collated, analysed, stored and published also needs to be determined. Where there is a desire to manage the BCM process using sophisticated software programs, great care needs to be taken to ensure that the selected applications match the requirements of the organisation. It is far too easy to invest in expensive commercial software packages that force an inappropriate BCM approach onto an organisation.

2.11 BCM program governance

The establishment of a governance structure for the BCM program should consider:

- How the development and implementation of BCM will be conducted and coordinated (for example a corporate BCM manager is appointed);

- How overall direction and drive for the program will occur (for example a steering committee will be appointed);
- How performance and achievement will be tracked (for example establishment of milestones and reporting requirements); and
- What sign-offs, approvals, authorisations, etc will be required at different stages of the program.

2.12 Summary

In summary the key issues in establishing the framework for BCM include:

- Creating an improved awareness and understanding in those involved in implementing or managing BCM, such as:
  - understanding what the organisation is about and what are the key things it is trying to achieve: (*critical business objectives*),
  - understanding uncertainty in the future (*the potential for disruption*),
  - understanding how the organisation achieves an effective implementation (*the processes, resources, dependencies and interdependencies*).
- Developing effective two-way communications with key stakeholders whilst the framework is being developed, and through its ongoing deployment.
- Creating and growing commitment to BCM in senior management and other key players.
- Establishing and resourcing appropriate structures for implementation and ongoing management of the BCM framework.
- Ensuring that appropriate governance is in place for the BCM program.

To assist in the implementation of the *Commencement* step, a checklist is provided at Section 2.13 and templates for information gathering at Section 2.14.

2.13 The commencement checklist

		Activity status				
Element	**Issue**	**Not started**	**Delayed**	**On targe**	**Completed**	**Comments**
Awareness and understanding	Has an appropriate awareness been developed of what is important for the organisation to achieve?					
	Have you identified key dependencies and interdependencies?					
	Have you examined past incidents, disruptions & losses?					
	Has the scope of the BCM program been developed?					
	Have key information sources been identified?					
Communications	Have key stakeholders been identified?					
	Have key information requirements been determined?					
	Have effective BCM program communications been established?					

Element	Issue	Activity status: Not started	Activity status: Delayed	Activity status: On targe	Activity status: Completed	Comments
Engagement and commitment	Has a plan been developed to gain/improve management commitment?					
	Is there an ongoing program in place to ensure that management commitment is sustained?					
	Have emotional triggers of management been considered?					
	Have requirements for the engagement of other staff been considered?					
	Have other stakeholders been identified?					
	Have the information needs of stakeholders & the organisation been considered?					
Resourcing	Has a business case been prepared and approved?					
	Has appropriate consultation been conducted during the preparation of the business case?					
	Are sufficient resources available for each step of the program?					
Program infrastructure development	Have management and governance arrangements been established?					
	Has an implementation/ management plan been developed?					
	Has a reporting framework been established?					
	Have performance indicators been developed?					

2.14 Example templates

Title or simple description of the critical business function or process

Identify what the function is trying to achieve, this may be based on minimum acceptable performance standards, KPIs,

Determine the importance of the function as ‘Gold’, ‘Silver’ or ‘Bronze’

Template 2.1
Identification of critical business functions

Critical business function or process	Physical location	Critical success factors	Functional interdependencies	Priority	Practical grouping
On call service assistance – region 1	Level 5 North Tower, New City	24 hour access to services 4 hour response business hours 8 hour response after hours	Region 1 and Central maintenance field crews Customer Help Desk Client services management team	High	On call service assistance functions for regions 2, 3 and 4.

Identify the location or locations where the activity is conducted

Identify key upstream and downstream interdependencies

Identify common groupings of critical business functions, for example those that may be suitable for the conduct of a combined single BIA

3 Assessing risks and developing disruption scenarios

3.1 What is risk?

Risk has traditionally been viewed as the bad things that can happen to us, and as something that insurance is meant to fix. Today, it is generally accepted that risk is a manifestation of uncertainty in our future, in particular risk represents the uncertainty in the outcomes of the decisions we make. Risk can therefore have both positive (benefits) and negative (disbenefits) outcomes associated with it. The joint Australian/New Zealand Standard* defines risk as:

'the chance of something happening that will have an impact upon objectives'

From a business continuity perspective it is often convenient to view risk as any source of disruption that may act as a barrier to the achievement of key business objectives. However, even apparently beneficial risks (the sudden collapse of a major competitor) can result in significant disruption (the sudden influx in new customers overwhelming capability and capacity to provide service).

3.2 Using risk assessment in BCM

Just as BCM is an integral part of good organisational *risk management*, the *risk assessment* is a critical step in the BCM process. The role of risk assessment within BCM is to provide a means of identifying and prioritising the types of event that could cause disruption to the organisation and give a broad indication of the consequences of such events and their likelihood. This provides the key inputs upon which subsequent business impact analysis can be developed.

** AS/NZS 4360: 2004*

The risk assessment step can also generate additional value to the organisation if it is approached with a broader risk management perspective to include the following activities:

- Identifying risks that may result in disruption to the achievement of business objectives;
- Undertaking qualitative or quantitative analysis to measure the level of risk;
- Prioritising these disruption risks and determining the organisation's tolerance to them;
- Determining the organisation's vulnerabilities to these disruption risks; and
- Providing outputs from the assessment to determine treatment strategies for managing these risks, pre- and post- incident, for example through:
  - avoiding activities that may result in unmanageable disruptions,
  - implementing process improvements,
  - instituting change management,
  - changing resource allocations,
  - developing business continuity and disaster recovery plans.

The Australian/New Zealand Standard (AS/NZS 4360:2004) provides a robust proven methodology for assessing and treating risks relevant to BCM (Figure 6).

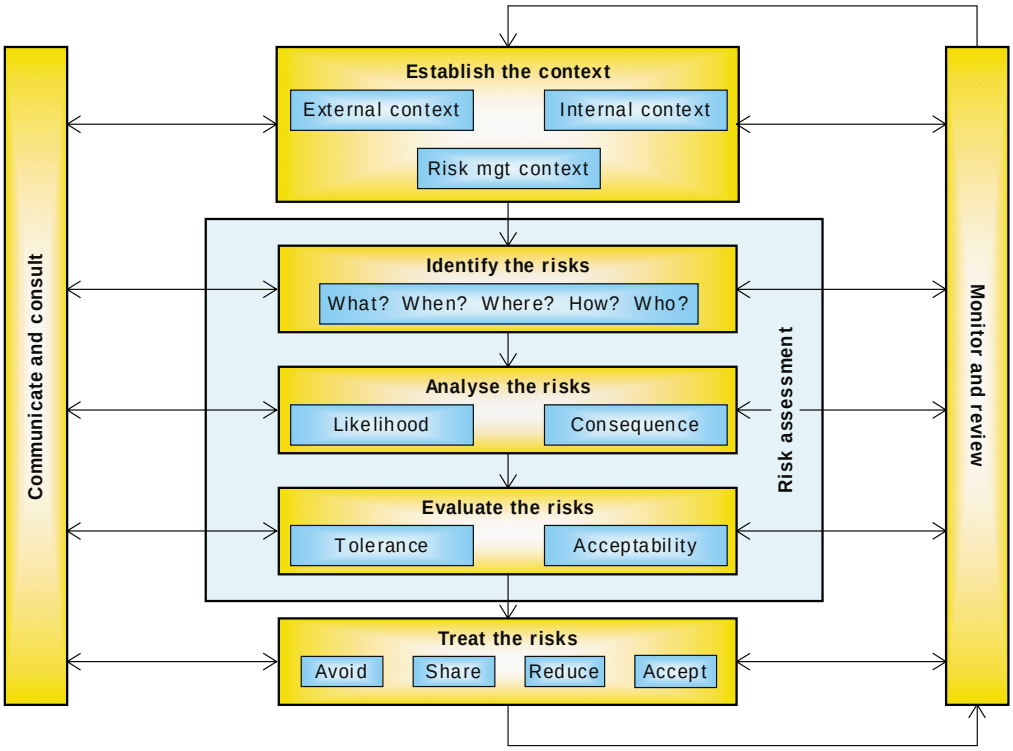


FIGURE 6 THE RISK MANAGEMENT PROCESS*

* based on AS/NZS 4360:2004

There are obvious synergies that can be exploited between an organisation's business continuity management activities and those of the risk management function. By liaising with risk managers, the BCM practitioner should be able to obtain a wealth of information for use in their own risk assessment process – saving time and resources for the organisation. A considerable amount of the risk assessment required for BCM may already have been undertaken by others, providing even more quality input into the process.

This has nothing to do with the debate about whether BCM should be part of risk management. It is about exploiting opportunities where useful skills, experience and knowledge are found elsewhere.

Furthermore, for the BCM practitioner to consciously expand the scope of the risk assessment to encompass a more through risk management process, treatment of disruption risk will start to become a focus of attention. This means that the practitioner can lead the creation of proactive improvements in capabilities in resilience. This should start to lead the paradigm shift away from the traditional approaches of 'just planning for them'. For this reason the following sections have a strong emphasis on conducting a robust risk management process as part of BCM, although the key elements of risk assessment as a stand alone are there for those who chose the more circumscribed approach.

3.3 Communicate and consult

The need to regularly communicate and consult throughout the BCM program is equally essential during the conduct of the risk assessment. Much of the information required to conduct a robust and comprehensive risk assessment will need to be sourced from others, some of whom may be external to the organisation. These third parties need to understand the context in which the risk assessment is being conducted and the types of information that is being sought if the appropriate information is to be gathered. Therefore, to achieve this, the communication needs to be a two-way dialogue.

There will be extensive synergies (in the process, players and information) between this risk assessment and other risk management activities conducted at a corporate level.

3.4 Establishing the context

Establishing the context involves gathering information and gaining a better understanding of the priorities and operations of the organisation, the nature of the environment within which it operates, and potential sources of disruption to these priorities and operations.

It is likely that a significant amount of information has already been collected and analysed during the '*Awareness and Understanding'* activities of the BCM process and in other risk assessments that may have been conducted previously, as part of BCM or other initiatives within the organisation. Figure 7 provides a summary of some of the issues and sources of information that should be considered in *Establishing the Context*.

Establishing the Context generally considers:

- The external context;
- The internal context; and
- The risk management context.

3.4.1 The external context

Developing an understanding of the external context involves considering how the organisation is currently, or potentially may be influenced by issues such as:

- ***The physical environment,*** for example: the potential for natural events such as floods, storm damage, heatwaves, droughts, earthquakes, etc;
- ***The built environment***, for example: loss of utility in infrastructure such as power supplies, communications networks, road networks, etc;
- ***The socio-political environment,*** for example: impacts of changing or new legislation, local community activities or demography, economic and social infrastructure changes, etc; and
- ***Industrial and market environment***, for example: changes in market structure and dynamics, competitive pressures, technological capability and sustainability, labour availability, suppliers and customers, etc.

3.4.2 The internal context

A good starting point in developing an understanding of the context is to commence with the organisation's objectives and determine those which are ***critical objectives***. It is important to realise that during a disruption it will not usually be possible to operate at a level such that all business objectives will be achieved. It will be necessary to prioritise and determine which objectives are critical to the ongoing success of the organisation through this disruption period.

Most of this information should have been identified and collated during the early establishment of the BCM program. However, revisiting it again at this stage provides an opportunity to refresh that analysis and examine the issues from different perspectives within the organisation.

This identification and acceptance of critical objectives should require input and approval from senior management and will often necessitate consultation with key stakeholders (eg customers and suppliers) to establish that these critical objectives are in line with their expectations or contractual requirements.

From an understanding of the critical objectives it should be possible to identify **critical business functions** (groups of processes) that are required to achieve those objectives. The 'acid test' to confirm a business function as 'critical' is to determine to what extent the critical objectives will be achieved if a particular function is 'removed'. Although some functions may not be appear to be critical in their own right, they may become regarded as critical because of the essential support they provide to other critical business functions.

Criticality of business functions is closely aligned to the potential length of any disruption. For example, during a two to four week disruption, customer service delivery may be regarded as critical over that period, whilst a function such as strategic planning would probably not. However, if a prolonged disruption of up to a year is considered then strategic planning may begin to be regarded as a critical business function.

3.4.3 The risk management context

Developing the risk management context, within the BCM process, is as simple as defining the scope and parameters for undertaking the risk assessment step. It is good practice to consider the following issues at this time:

- Confirming the objectives of the risk assessment (for example 'identify and prioritise risks that could prevent the continued access to the Customer Service Centre');
- Physical, structural, functional and infrastructural elements that are included in the risk assessment (for example '*all manufacturing operations within co-located Plants A & B'*);
- Specific exclusions (for example 'regional offices are not to be included');
- Data and information sources for inputs into the risk assessment (for example 'plans, reports and other documentation from operational areas, planning, support functions, internal audit, risk, and emergency management');
- Risk assessment methodologies and expertise required to conduct the assessment (eg 'using the corporate risk assessment toolkit with a risk workshop facilitated by the risk manager');

- Agreed responsibilities and accountabilities for the risk assessment (eg 'the BCM coordinator will be responsible for….., the General Manager procurement will be accountable for…..';
- Resources to be deployed in the risk assessment (eg 'managers 'a',' 'b, & 'c' to participate in a risk workshop for two hours'); and
- Deliverables and expected outcomes, (eg the assessment will be carried out 'according to the following timelines and delivery dates'; 'a risk assessment covering all outreach business units will be provided to level 1 and level 2 managers for review').

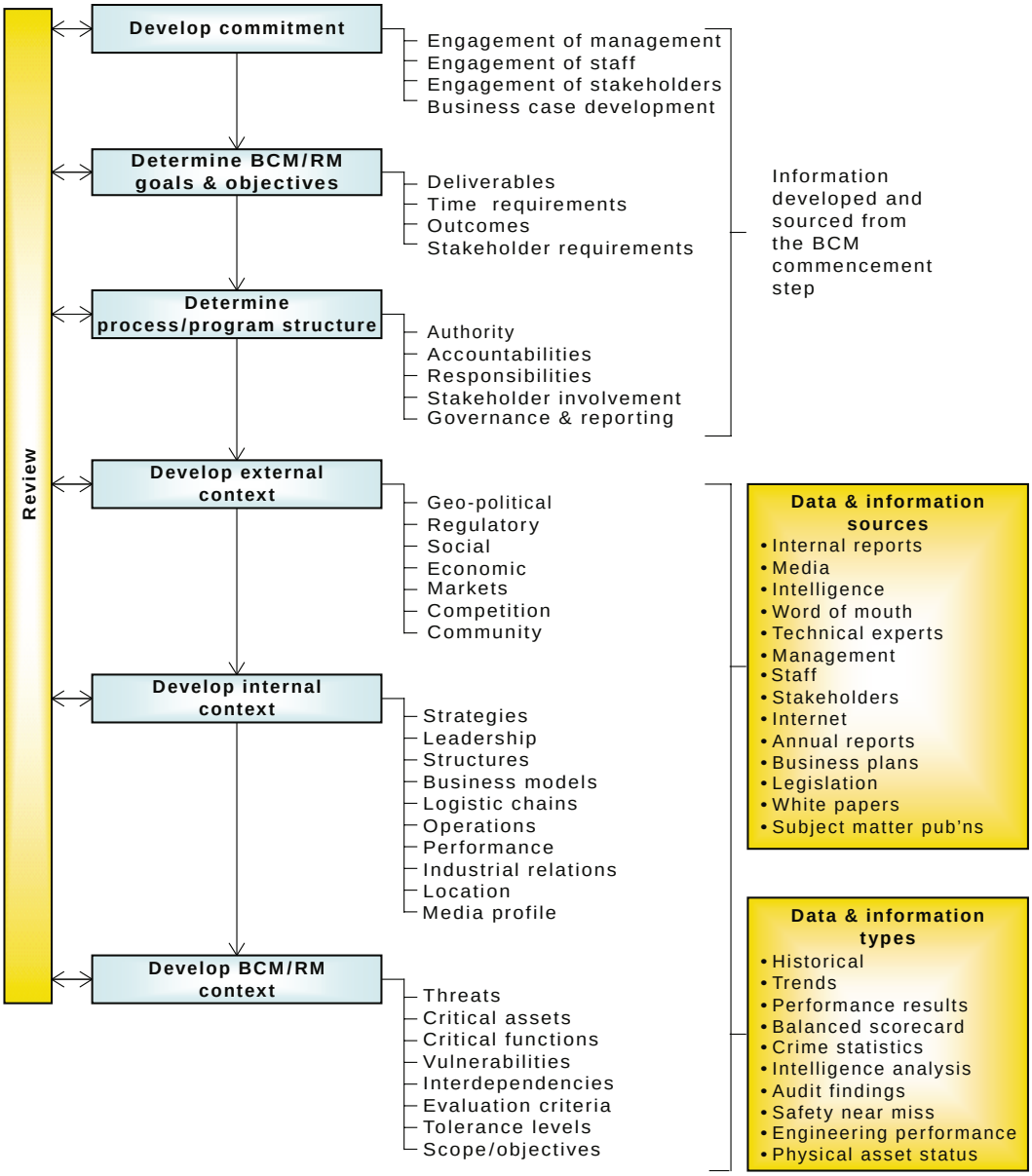


FIGURE 7 ACTIVITIES AND INFORMATION SOURCES IN ESTABLISHING THE CONTEXT*

* Source: adapted from *Security Risk Management Handbook, Standards Australia*, in preparation 2006.

3.4.4 Developing the evaluation criteria

An important outcome of the risk assessment will be the measurement and prioritisation of risk. Risks are evaluated against one or more criteria, which are developed at this stage.

Criteria that need to be considered include:

- **Consequence:**
  - the types of consequence that will be assessed, for example financial, reputational, safety, people, community impacts, etc,
  - any measurement of the level of consequence that will be applied.
- **Likelihood:**
  - how likelihood will be determined, eg probability, frequency of occurrence, etc.
- **Relationships and evaluation:**
  - how the relationship between consequence and likelihood can be used to generate a measure or description of risk (for example, creating a likelihood versus consequence rating matrix).
  - how particular levels of risk will used to determine priorities, acceptability, tolerability, the need for treatment (eg development of a BCP, etc).

3.5 Identifying risk

There is often confusion between the terms ‘hazard’ and ‘risk’. Hazard is defined as a ‘*source of potential harm’*. Hazards may be present without a risk being created. For example, a sharp knife can be a hazard. If left on a tall shelf it will still be a hazard, but would not represent a risk to small children who could not reach it. However, if the context changed: eg the shelf was lower, or a child was taller then a risk of injury through a knife cut could be created.

In identifying risk, one of the first steps is to identify existing or potential sources of risk. These may be represented by hazards (in both the traditional safety sense or as business disruption hazards) or threats (as in the security or business sense). From this point, a more detailed examination of the causes (eg root causes such as the absence of suitable storage for kitchen knives) can be conducted.

In addition to its source, risk is characterised by:

- The potential occurrence of some future event (for example *the child takes hold of and plays with the knife*);
- A potential consequence of the event (for example the child cuts herself and requires hospital attention);

- The likelihood of the event occurring **with** that consequence (for example it is likely she will play with the knife and in doing so will cut herself severely); and
- The absence or presence and effectiveness of controls (for example she cannot reach the shelf, the stool is locked away, she has been taught not to play with knives).

To adequately describe a risk it can be convenient to consider the following elements:

Adequate risk description	=	Description of the event	+/-	Description of consequence	+/-	Description of controls

Where if any ***two*** or more of the descriptors (event, consequence or controls) are present then a risk is probably being described, if only ***one*** of the descriptors is present then it more likely that a hazard or threat, rather than a risk is being considered.

In seeking to identify possible sources of risk the *Risk Arena* (Figure 8) provides a useful *aide memoire* to ensure that a comprehensive range of sources is considered. The *Risk Arena* presents sources of risk external to the organisation in the outer circle, whilst potential sources of internal risk are presented in the inner circle. A more comprehensive checklist, based on the risk arena, for identifying sources of risk is provided at Appendix B (further examples of specific threats and hazards are at Appendix D).

It is vitally important to remember that much of our thinking on risk is based upon, and biased by our and others' perceptions. Truly objective consideration is often a rare commodity. There are likely to be many different viewpoints of what 'reality' really looks like, thus emphasising the importance of involving others in the risk assessment process. An effective consensus approach not only improves ownership and buy-in to the risk assessment, it should also provide a more 'realistic' result. Perception can reinforce bias in a range of activities, including:

- Selecting data and information;
- Determining the validity and accuracy of, and the trust in sources of data and information;
- Differential weighting, or importance of data during analysis;
- Assessing the relevance, validity and acceptance of the products of analysis;
- Decision making on the appropriate treatment of risk; and
- Decision making on the relevance of changing context.

A variety of factors will create and change perception in those parties involved in the risk assessment process:

- Personal experience of past events;
- Perceived extremity or severity of event;
- Perceived likelihood of event;

- Recognition and acceptance of threat or hazard;
- Degree of control over the risk;
- Dread & fear of the risk and its consequences;
- Proximity of impact to the person's 'world';
- Cueing, through the media, colleagues, etc; and
- Existing beliefs, emotions and values.

A more thorough discussion of perception of risk is presented in Chapter 8.

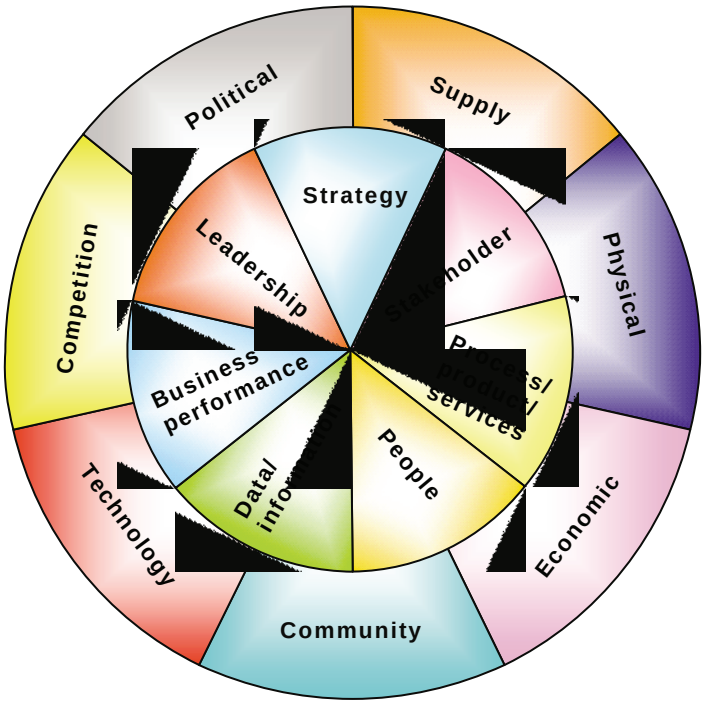


FIGURE 8 THE RISK ARENA*

- There are a variety of techniques that can be employed in the identification of risk including:
- Hazard tree analysis;
- Brainstorming in team or workshop environments;
- Systems analysis;
- Delphi technique;
- Hazard and operability (HAZOP) studies;
- Structured interviews;
- Questionnaires; and
- Case study analysis.

Whatever approach is adopted, there are a number of questions that should be posed:

---

* *Trident: Security Risk Assessment 2001, reproduced with permission of Executive Impact Pty Ltd.*

- **What:**
  - what could happen?
  - what could the effect on objectives be?
  - what is in place to stop it from happening?
  - what is in place that may promote it happening?
- **How:**
  - how could it happen?
  - how would we know it was happening?
  - how resilient are we if it happens?
- **Where:**
  - where could it happen?
- **When:**
  - when could it happen? Any time periods of particular sensitivity?
- **Who:**
  - who could be involved?
  - who could be affected?

At this stage all risks identified should be documented, even those that at first may seem to be unimportant. As the program proceeds, these risks could change in importance and may need further consideration for treatment.

3.6 Analysing risk

Analysing risk is about developing an improved understanding of the risk. It involves developing information that will enable the relevant importance of different risks to be judged against each other and to assist in decision making on the need for treatment of those risks.

One of the commonest methods of analysing risks is based upon the measurement of ***consequence*** and ***likelihood*** using either qualitative or quantitative approaches.

Consequence and likelihood are determined in the full consideration of the effectiveness of controls present. The vulnerability analysis provides one approach for examining the effectiveness of controls with respect to defined sources of risk.

3.6.1 The nature of vulnerability

The concept of vulnerability is based upon the organisation's capability to withstand the impacts of the disruption risks and the degree to which these risks are not capable of being managed. Information on the presence and absence of controls can be used to provide an indication of the organisation's vulnerability to these disruption risks. An assessment of vulnerability can help to identify areas where risk treatment needs to be developed proactively and to what extent BCM strategies will need to be developed. Broadly, there are four areas for which vulnerability needs to be considered:

- The vulnerability of people contributing to the organisation's critical objectives;
- The vulnerability of information essential to achieving the critical objectives;
- The vulnerability of facilities, assets and other infrastructure required to support the critical objectives; and
- The vulnerability of processes that utilise these three key types of resource.

Vulnerability is an extension of the consideration of control effectiveness, where in effect one is related to the inverse of the other. Thus lowering the control effectiveness will tend to elevate the vulnerability.

A simple (approximate) vulnerability assessment can be undertaken by a straightforward extrapolation of the examination of control effectiveness undertaken during the risk assessment; eg where high control effectiveness would equate to low vulnerability and vice versa. However, using this approach needs to be treated with some caution as a very small reduction in control effectiveness could result in a significant increase in vulnerability in some circumstances.

A more through approach involves undertaking a detailed separate vulnerability analysis using the outputs from the risk analysis. This is done by considering for each key risk scenario the way in which the presence and absence of controls will create or remove vulnerability for people, information, property or processes. A variety of factors can be used to assess the level of vulnerability using this approach (Table 3). Examples of issues that could be considered in conducting a vulnerability analysis are included in Appendix E.

Table 3
Example of vulnerability analysis rating levels

Vulnerability rating	Indicators of vulnerability
Very high	• Presence of controls is limited to exceptionally few parts of the organisation. • Recent evidence of widespread control failures. • Controls &/or mitigating strategies have never been reviewed. • Controls &/or mitigating strategies are currently completely ineffective. • Almost certain that controls will fail during a disruption. • Highly likely that severe disruptions to the organisation will occur. • Extreme losses result from a small deterioration in controls.
High	• Few controls &/or mitigating strategies are present in critical business functions. • Recent evidence of significant control failings. • Controls are reviewed on an ad hoc and infrequent basis. • Controls &/or mitigating strategies are largely ineffective. • Highly likely that controls will fail during a disruption. • Significant disruptions to the business are expected. • Major losses result from a small deterioration in controls.
Moderate	• Some controls &/or mitigating strategies are present in critical business functions. • Recent evidence of a small number of controls failing. • Key controls &/or mitigating strategies are reviewed on a frequent basis. • The majority of controls &/or mitigating strategies are adequate to manage the disruption. • Possible that some controls will fail during a disruption. • Some disruption to the business is expected. • Moderate losses result from a small deterioration in controls.
Low	• Controls &/or mitigating strategies are present in all critical business functions. • There are no recent examples of controls failing. • Majority of controls &/or mitigating strategies are reviewed on a frequent basis. • Controls &/or mitigating strategies are largely effective. • Unlikely that controls will fail during a disruption. • Little disruption is expected. • Minor losses result from a small deterioration in controls.
Very low	• Comprehensive controls &/or mitigating strategies are present in all critical business functions. • There have been no previous control failings. • Continuous monitoring and review of controls is undertaken. • Controls &/or mitigating strategies are optimum and are sustainable. • Rare that controls will fail during a disruption. • No material disruption is expected. • Negligible losses result from a small deterioration in controls.

3.6.2 Determining consequence

AS/NZS 4360:2004 defines consequence as:

'outcome or impact of an **event**'

It is important to remember that:

- An event can demonstrate more than one consequence;
- Consequences can be both positive and/or negative; and
- Consequences should be considered with respect to the achievement of the defined objectives (eg 'corporate', 'business', 'project', 'unit', 'personal', 'critical', etc);

Types of consequence that could be considered (depending upon the identified critical business objectives) include:

- Financial

For example, lost production capability, lost sales, increased costs of working, market loss, contractual penalties imposed, physical damage, etc.

- **Reputational**

For example, harm to brand & image, loss of stakeholder confidence, unwelcome media attention, loss of goodwill, etc.

- **Stakeholder**

For example, service level agreement compliance, service & product delivery, accessibility, payment capacity, satisfaction levels, etc.

- **Social and community**

For example, loss of utility experienced by the local community, collateral damage to community assets, loss of local economy, health & welfare impacts within the community, etc.

- **People**

For example, stability and productivity of the workforce, health and welfare of the workforce, continued employment capability, voluntary exit of key staff, etc.

- **Operational**

For example, productivity, process availability, market share and position, plant capacity, etc.

- **Regulatory**

For example, compliance levels, regulatory actions & penalties, intervention by regulators, etc.

In most circumstances consequence arising from a potential disruption event should be determined on the basis of 'most credible worst case scenario'. The ultimate *worst case scenario* of many risks could potentially be an *immediate* total catastrophic loss and collapse of the organisation. However, such extreme worst case scenarios are not those that are experienced by the vast majority of organisations that are exposed to risks of business disruption. It is usually most appropriate to use available historical precedent to determine realistic worst case losses that could be expected from a particular disruption risk (hence the 'most credible' scenario).

In practice it can often be difficult to gain an accurate estimation of the level of consequence arising from a potential disruption event, in particular for high consequence – low probability events which are outside of common experience. It is in such circumstances that one is more likely to experience widely different perceptions of the issues. An *example* of one approach to measuring the potential consequences of an event is provided in Table 4. When estimating consequence, this should be done in *full consideration of the effectiveness of controls already in place*.

Table 4
Example of consequence measurement criteria

Consequence rating	Consequence		
	Financial	**Reputational**	**Project/business**
Catastrophic	• Operating budget blowout of >30%. • Reduction in operating profit of >30%.	Extreme negative coverage, public outcry appearing consistently over weeks. Majority of stakeholders severely disadvantaged (months).	Serious process breakdown that prevents the achievement of mission critical objectives.
Major	• An operating budget blowout of 20-30%. • Reduction in operating profit of 15-30%	Negative significant coverage, appearing consistently over weeks. Multiple stakeholders severely disadvantaged (weeks - months).	Serious process breakdown that substantially impedes the achievement of a core objective.
Moderate	• An operating budget blowout of 5-10%. • Reduction in operating profit of 5-15%.	Negative coverage lasting for several days, and/or frequent re-occurrence for several weeks. Multiple stakeholders experience significant disadvantage (weeks).	Process breakdown that impedes the achievement of an important objective or causes extensive inefficiencies in key processes.
Minor	• An operating budget blowout of 1-5%. • Reduction in operating profit of 1-5%.	Minor negative coverage, limited circulation for one day. Minority of stakeholders experience disadvantage (days - weeks).	Process breakdown that impedes the achievement of an important objective or causes some inefficiencies in key processes.

(*continued*)

Table 4 (*continued*)

Consequence rating	Consequence		
	Financial	**Reputational**	**Project/Business**
Minimal	• An operating budget blowout of <1%. • Reduction in operating profit of <1%	Isolated brief coverage, single media outlet. Stakeholders experience minimal disadvantage (days).	Process breakdown or inefficiencies that have a limited impact on the achievement of an objective.

3.6.3 Determining likelihood

Likelihood refers to the chance or probability of an event occurring *with those specific defined consequences*[*]. The likelihood can be expressed in a variety of ways, for example: as an absolute probability (eg occurring with a probability of between 0 and 1); as the chance that something will occur over a defined period (eg 'over the next two years'); or as a percentage chance of occurrence. An example of one approach to measuring likelihood is provided in Table 5. Estimation of likelihood is based on a consideration of the *effectiveness of the controls known to be currently in place*.

Table 5
Determining likelihood

Likelihood	Criteria
Almost certain	• Over 99% probability, or† • "happens often", or • could occur within 'days to weeks'
Likely	• >50% probability, or • "could easily happen", or • could occur within 'weeks to months'
Possible	• >10% probability, or • "could happen, has occurred before", or • could occur within 'a year or so'
Unlikely	• >1% probability, or • "has not happened yet, but could", or • could occur 'after several years'
Rare	• <1% probability • "conceivable but only in extreme circumstances" • exceptionally unlikely, even in the long term future • a '100 year event' or greater

* Note this is not just the *likelihood of the event* occurring.

† Use of probability needs to be carefully defined in each case that is used, e.g. probability of an armed robbery occurring over a defined number of armoured car journeys.

3.6.4 Determining the risk level

The overall level of risk or *risk rating* can be determined through combining the consequence and likelihood estimations, an example approach is provided in Table 6. This approach provides a potential range of ratings from *Low* to *Extreme*.

Table 6
Example of a Risk Rating Matrix

		Consequence				
		Minimal	**Minor**	**Moderate**	**Major**	**Catastrophic**
Likelihood	**Almost certain**	Medium	Significant	High	Extreme	Extreme
	Likely	Medium	Medium	Significant	High	Extreme
	Possible	Low	Medium	Significant	High	High
	Unlikely	Low	Low	Medium	Significant	High
	Rare	Low	Low	Medium	Significant	Significant

3.7 Evaluating risk

Evaluating risk involves determining which risks are acceptable (or can be tolerated), and which risks are unacceptable (or cannot be tolerated). An initial set of criteria for determining acceptability/tolerability will usually have been developed whilst '*Establishing the Context*'. However, at this stage it is appropriate to review and validate these evaluation criteria in light of the results of the risk analysis and any subsequent changes in Context that may have occurred. The organisation's tolerance for risk could, for example, be based upon decisions such as:

- **All risks of 'Extreme' rating** - are unacceptable, treatment of the risk, for example through risk control improvements, should be an immediate high priority;
- **All risk above a 'Significant' rating -** where controls are less than 'Adequate' – may be considered intolerable, requiring an assessment of potential treatment options;
- **Any risk below a 'Medium' rating** - where control effectiveness is 'Adequate' or better may be regarded as 'Tolerable' and should be monitored for any future change in status; and
- Any risk with a residual (post treatment) consequence above moderate requires consideration for BCM.

3.8 Treating risk

There is a common misconception that the only treatment that is required in BCM is the development of the business continuity plan. This view misses out on a significant opportunity to proactively enhance the resilience of the organisation to future disruption. Any decisions on treatment of intolerable risk needs to consider a range of other options in addition to the writing of plans. On many occasions planning may be the primary or only feasible treatment option. However, it should also be considered as a further treatment for residual risk remaining *after* other treatments have been implemented, particularly where the residual risk may be of high consequence (eg where likelihood has been reduced following other treatments). An approach for treating disruption risks is summarised in Figure 9.

The choice of treatment can be guided by the profile of the risks, i.e. by mapping the position of each risk onto the risk matrix. Figure 10 provides an example of such mapping as an aid to treatment decision making.

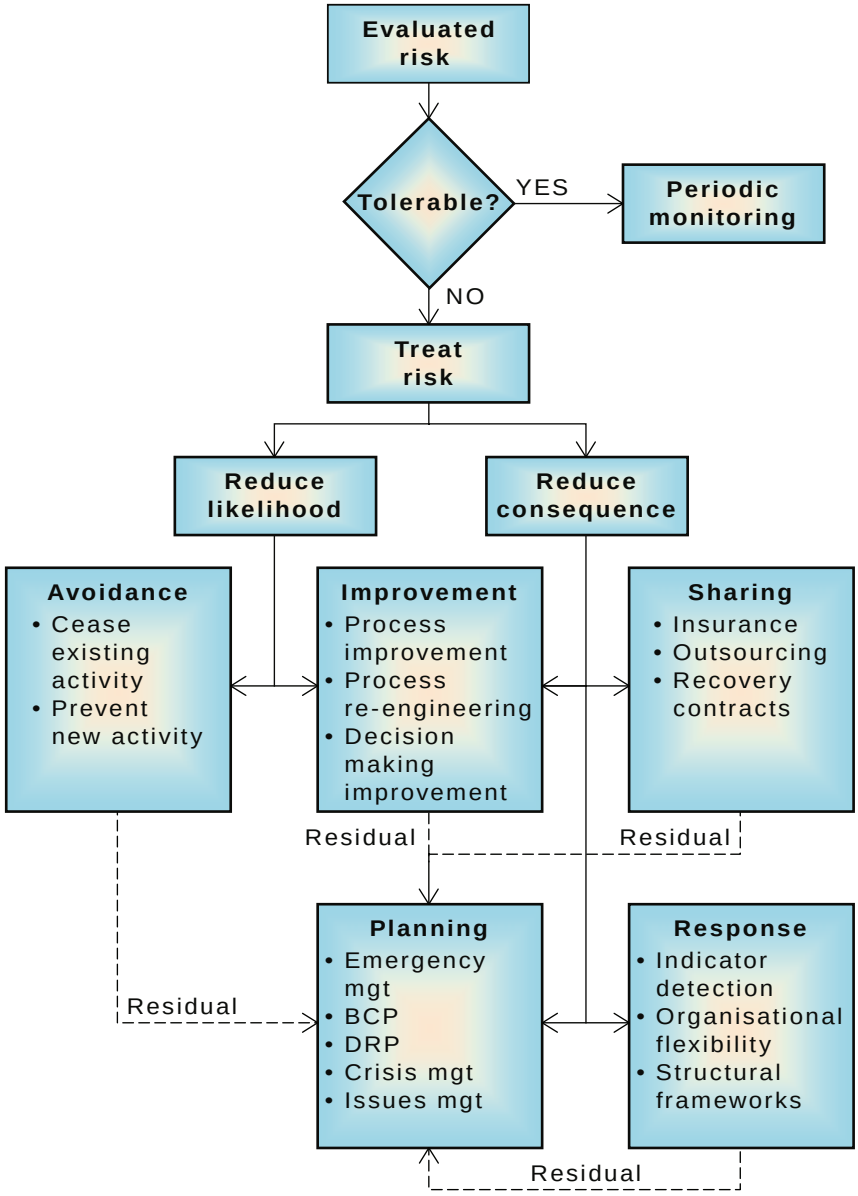


FIGURE 9 EXAMPLES OF TREATMENT OPTIONS

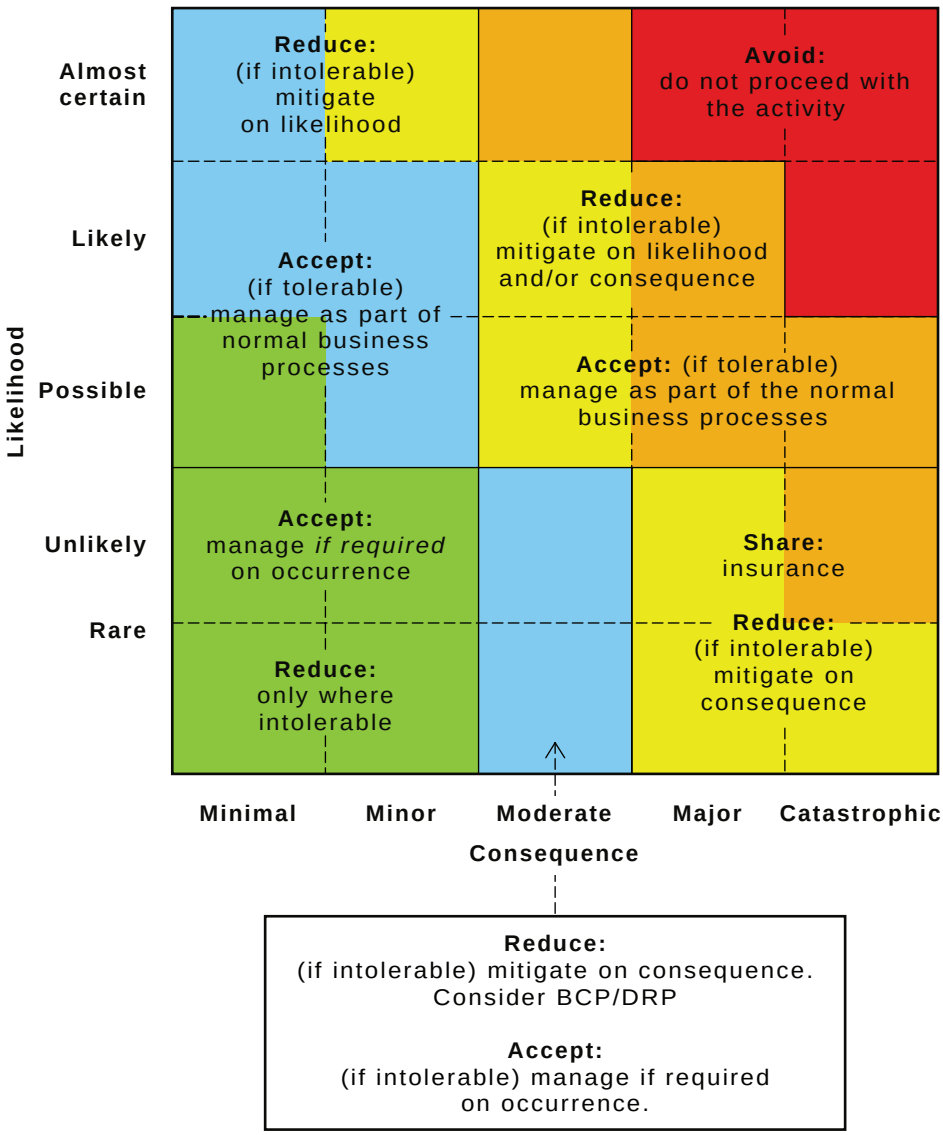


FIGURE 10 DECIDING UPON THE TREATMENT STRATEGY

3.9 Monitor and review

Following the implementation of treatments, there will still be an ongoing need to monitor and review the level of disruption risks and the ongoing effectiveness of any risk controls and treatments. There should at all times be a strong emphasis on:

- Continuously re-examining the *Context* and reconsidering its effect on risk and any subsequent disruption scenarios;
- Verifying the appropriateness of the findings of the risk assessment in light of any changes to the context; and
- Assessing the efficiency and effectiveness of treatments (including BCPs) in mitigating the risks identified and re-evaluation of their appropriateness.

3.10 Developing disruption scenarios and dealing with uncertainty

The risk assessment can produce a large number of specific disruption risks. Trying to use this volume of information as the basis for the BIA and for subsequent planning can be a daunting and unnecessary task.

There is therefore a need to consider further developing the outputs of the risk assessment to both simplify the conduct of the BIA and to improve the flexibility and relevance of its outputs. It can often be more effective to group risks into broader risk scenarios (or 'meta' risks) on which to base the BIA and subsequent development of plans. Consider the following hypothetical outputs from a typical risk assessment (these outputs are in effect hazards or sources of risk):

- Fire;
- Flood;
- Power failure;
- Industrial dispute;
- Chemical spill;
- Construction works;
- Bomb hoax;
- Storm damage; and
- Failure of building access controls.

If a full description of risk is developed for each of these, for example:

'a fire in the building results in loss of access to the building for greater than 24 hours',

'storm damage to the building's utilities results in loss of access to the building for a period in excess of 24 hours'

…it becomes apparent that irrespective of the cause or nature of the specific event, there will be a common impact on the organisation:

'*following a disruption event, access to the building is denied for a period in excess of x hours*'.

This actually provides us with a suitable consolidated risk description or risk scenario against which the BIA and planning can be subsequently developed. Thus instead of creating individual plans for each specific risk, it is possible to develop a single plan that considers the requirements for managing a much broader disruption scenario: the risk of loss of access to the building (Figure 11).

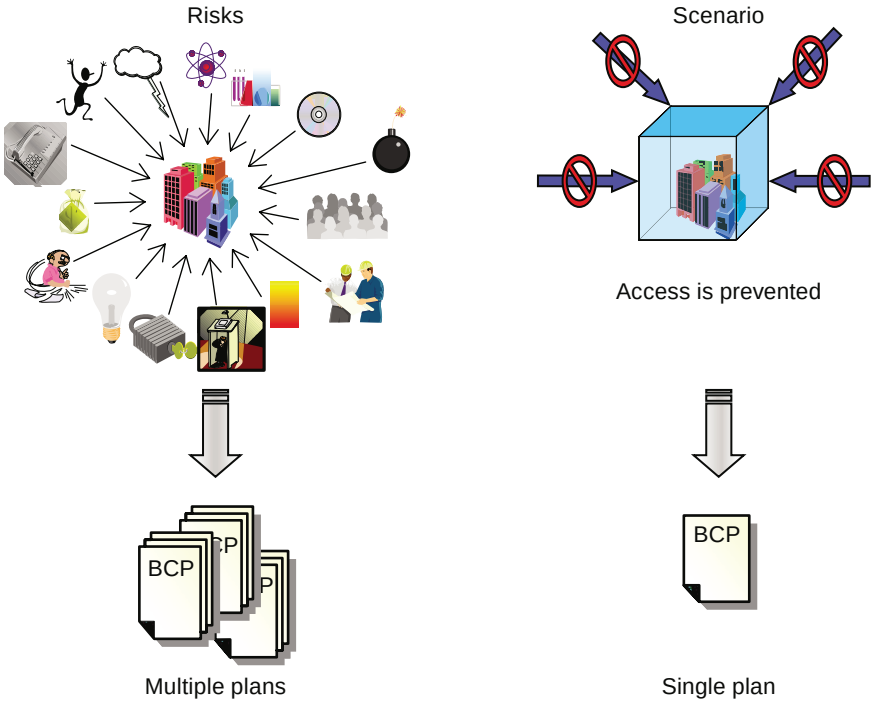


FIGURE 11 ALIGNING RISKS IN SCENARIOS

In deciding if the business impact assessment (BIA) and subsequent planning should be carried out to manage individual risk events or consolidated risk scenarios, consideration of the following points may prove to be valuable:

- **Dissociation**

Actual disruptions are rarely typified by the description of the risk that precedes them. Therefore plans (developed to manage specific risks) may have little similarity to the event that occurs, creating *irrelevance*.

- **Singularity**

Multiple risks may be typified by the same single type of impact upon resources, processes, people and infrastructure. Therefore multiple plans may be created all of which address the same issue following an event, creating *redundancy*.

- **Multiplicity**

A single risk may have multiple different effects in different parts of the organisation. Therefore plans may not cater for the range of impacts requiring management, creating *insufficiency*.

- **Concatenation**

Apparently disparate risks may combine to create a completely different type or range of impacts. Therefore plans may not be appropriate for the magnitude or diversity of the impacts requiring management, creating *inadequacy*.

- **Escalation**

The impact of an event may escalate over time, such that consequence increases or is more prolonged in duration than described in the risk. Therefore plans may not be capable of responding to a changing or worsening situation, creating *inflexibility*.

3.11 Summary

In summary the key issues associated with undertaking the risk assessment are:

- Risk is the chance of something happening that will have an effect upon objectives.
- BCM should be part of integrated risk management. The risk *assessment* process is a fundamental step in BCM.
- AS/NZS 4360: 2004 provides a robust process for undertaking the risk assessment.
- A vulnerability assessment is conducted to determine the organisation's capabilities to manage the identified disruption and identify areas where improvement (for example process improvement) or BCM strategies may be required.
- Two-way communication is an essential part of risk assessment, which includes appreciating the effects of perception on the delivery, receipt and analysis of information.
- Key outputs of the risk assessment are the determination of treatments for intolerable risks and the development of potential disruption scenarios, for use in subsequent business impact assessment.

To assist in the implementation of the *Risk Assessment* step, a checklist is provided at Section 3.12 and templates for information gathering at Section 3.13.

3.12 The risk assessment checklist

		Activity status				
Element	**Issue**	**Not started**	**Delayed**	**On target**	**Completed**	**Comments**
Establishing the context	Have the appropriate information resources been sourced?					
	Have appropriate documents and other information sources been reviewed?					
	Has the scope of the risk assessment been determined and approved?					
	Have evaluation criteria been developed?					
Risk identification and analysis	Have sources of potential disruption risks been identified?					
	Have risks, their impacts and likelihoods been identified and assessed?					
Risk evaluation	Has the level of risk and the organisation's tolerance to the each of the higher priority risks been determined?					
Disruption scenarios	Have disruption scenarios been developed from the identified risks?					
Vulnerability analysis	Have organisational vulnerabilities to the risks/scenarios been identified?					

3.13 Risk assessment templates

Identify potential disruption causes and contributing factors

Determine the overall consolidated risk or risk scenario

Determine the level of risk from the consequence and likelihood

Identify vulnerabilities to the risk existing in people, property, information, or processes.

Identify gaps in current controls or treatments that need to be addressed

Template 3.1
Disruption risk register

Risk sources *(What are the potential causes and contributing factors)*	Risk *(Including detailed description of the risk)*	Overall disruption risk/ Risk scenario	Risk assessment			Existing controls or strategies	Vulnerabilities	Treatments		Responsibility
			Consequence	Likelihood	Risk rating			Being Developed	Need to be developed	
Loss of external power. Damage to supply infrastructure. Building cabling/power control, failure.	**Power loss** Loss of power supply results in loss of: lifts, A/C systems and building access control for a period of greater than eight hours.	Loss of building access	Major	Possible	High	Back up generator on auto switch, capacity for critical floors only	Ageing electrical infrastructure within building. Floors 1 to 11 without backup power supply. No alternate site arrangements.	Mutual aid agreement with Acme organisation for use of 10 seats	Upgraded back up generator to provide power to 30% more of operation	GM Corporate Services.

Describe the risk with its associated impacts

Assess the consequence should the disruption occur

Assess the likelihood of a disruption with that consequence thoccurring with that consequence

Describe existing controls or strategies that would mitigate the risk

Describe treatments commenced but not yet not yet implemented

Identify the person/ position responsible for the risk & its treatment(s)

Identify locations impacted or included within the scope of the assessment

Describe the key overall impacts on each critical business function

Determine requirement for an update or development of new BCP

Template 3.2
Disruption scenario register

Overall disruption risk/ risk scenario *(obtained from Column 3 of Risk & Vulnerability Register)*	**Location(s)** *(where specific sites are involved)*	**Critical business function**	**Impact on business operations** *(describe the overall impact to the successful operation of your business and the key business functions affected)*	**BCP status**	
				Current	**Required**
Loss of access to IT systems	Level 8, North Tower, Capital City	Financial transactions	Transaction cannot proceed without access to financial data. Accounts payable, accounts receivable and financial reporting cannot proceed. Integrity of financial data may be compromised	✓ **8 Jan 2005**	✓ Update

Determine Critical Business functions at each location

Identify if a current BCP is in place and the date of its last update

4 Conducting the business impact analysis

4.1 What is the business impact assessment?

The business impact assessment (BIA) provides an analysis of how key disruption risks could affect an organisation's operations and what capabilities will be required to manage them. The BIA comprises six steps (Figure 12) that provides the 'BCM manager', 'BC planner' and the 'owners' of business functions with an agreed understanding of:

- How they contribute to the achievement of critical objectives;
- The key resources that are in place currently to achieve these critical objectives (eg people, processes, information and other infrastructure);
- How the risks or disruption scenarios will impact upon the capability of, and access to these key elements;
- The minimum acceptable level of operation to achieve these objectives and the minimum acceptable resource capability and availability required;
- Nature of interdependencies and how they will be affected by the disruption; and
- The BIA representing a significant voyage of discovery for many organisations and therefore needing to be an iterative process – as the discoveries of later steps may challenge the status of preceding steps.

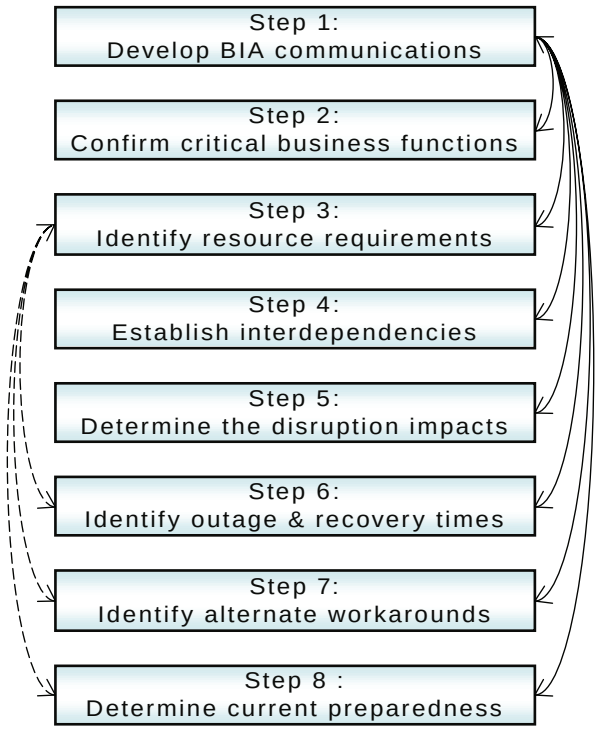


FIGURE 12 THE BUSINESS IMPACT ASSESSMENT PROCESS
(dotted lines represent information flows)

4.2 Step 1: Developing Communications for the BIA

For many people within the organisation, the BIA may represent their first real exposure to BCM activities. This involvement can represent a challenge and discomfort to the managers and staff involved for a number of reasons:

- Discussion will focus on the operation of key processes and will require those involved to have an appropriately relevant and detailed knowledge. It is surprising how many process owners and operators have little of such understanding and so can feel threatened by the questions posed by the BIA;
- The BIA focuses on aspects of structural and functional resilience. Again managers and staff may feel threatened and be unwilling to reveal too much regarding the fragility of processes and infrastructure under their control; and
- There will be an analysis of ‘normal’ resourcing levels compared with levels of resources that really are needed if there was a disruption. This can lead to a perception that ‘excess’ resources are being identified, that could subsequently be lost to the function.

It is thus essential that a two-way approach to communication during the BIA is carefully considered before proceeding (see Table 7).

Table 7
Communication and the BIA

Issue	Example approaches
Awareness: Management and staff need to be aware of the BIA, how it will be conducted and how its information will be used.	• Conduct a short awareness session (10 minutes) during a team meeting on the BIA to introduce broad concepts to management and staff. • Publish a short article in in-house publications (paper or electronic) providing key points and a schedule of BIA activities. • Produce a short (3-4 slides) presentation and notes as 'team-talk' to be presented by team managers. • Provide a short (less than a page) briefing note to be provided to each individual participating in the BIA.
Understanding: Management and staff need to understand:	
• The BIA process and time lines. • How it will be used to develop strategies and plans. • What information will be required. • How to record information and conduct any analysis required.	• Provide a short (<20 minute) training session on the BIA to teams at the start of the BIA process (eg at an opening workshop). • Make the training presentation available as both hard copy and as a visual presentation (eg PowerPoint presentation, or equivalent). • Provide one-on-one training where team/workshop training is not suitable.
Responsibilities and accountabilities within the BIA process.	
Commitment and trust: Management and staff need to recognise the need to undertake the BIA, have confidence in those conducting the BIA and have trust that information they provide will not be misused.	• Ensure that all relevant managers and staff are aware of the process and have an appropriate level of understanding of what is required. • Be available to answer question on the process. • Ensure that all answers and other information are provided in a timely and consistent manner. • Have appropriate information security/confidentiality procedures in place. • Ensure that process and escalation procedures are in place to address concerns as soon as is practicable. • Overall be as open as possible and demonstrate at every opportunity and with every action that there are no hidden agenda.
Effectiveness: The communications need to reach the appropriate audience at the right time, in the right manner and address the audience's and the BIA's needs.	• Before starting the BIA have a clear understanding of what is expected/required and how it can be measured. • Ensure that a process for monitoring the effectiveness of the BIA is in place from the start. • Record and report on the effectiveness of the communications, it will ensure they remain a strong focus throughout the BIA.

4.3 Step 2: Confirming critical business functions

In the earlier stages of the BCM, the critical objectives of the organisation will have been identified. From these, an initial identification of those business functions that contribute to each of the objectives will have been made. This in turn will have assisted in identifying those individuals that need to participate in the BIA. The next step of the BIA is to validate these business functions, with the selected managers and staff, and confirm which constitute *critical* business functions requiring consideration in the BCM process. This will lead to some critical business functions being modified, expanded, contracted, removed, or added.

The definition of what constitutes a critical business function will depend upon the Context within which the BCM is being conducted. Examples of some criteria are:

- The removal or loss of the business function prevents the achievement of the critical objective.
- Deterioration of the business function impairs achievement of the critical objectives to an unacceptable level.
- Loss or impairment of the business function for a period of greater than 3 days is unacceptable for the achievement of the critical objective.
- Loss of the business function for a period greater than 24 hours is unacceptable to priority customers.

The concept of *critical business function* in some contexts will encompass other critical infrastructure (eg critical assets such as core plant equipment).

As part of this validation process, critical success factors for critical business functions can also be determined. The critical success factors are the essential activities, deliverables or outputs that demonstrate that an appropriate level of operation is being achieved. Critical success factors will often be defined under service level agreements.

The outcome of this step of the process should be the identification of, agreement on, and documentation of the critical business functions and the key processes that contribute to them. It is worthwhile seeking senior management endorsement of the identified critical business functions before proceeding to the next step.

4.4 Step 3: Identify resource requirements

In this step the current level of resourcing for each critical business function is identified to determine current capabilities and the potential for future spare capacity or shortfall. It should cover for example the type, number, location, etc of the following resources:

- **People**

Managers, staff, contractors and consultants currently contributing to the critical business function. Include key roles and responsibilities for each individual, locations, contact details, deputies for each position, etc.

- **Facilities**

Identify types of facilities in use currently (for example: '3 workstations in open office, 1 manager's office, 1 meeting room').

- **Equipment**

Identify general office equipment, telecommunications, and any specialised equipment in use (for example *computers, filing cabinets, cameras, photocopiers, plant machinery*).

- **IT systems**

Identify IT systems and applications currently in use.

- **Information**

Identify current information requirements (for example required *paper records, electronic documents*).

- **Budget**

Identify current budget, cash flow, expenditure and/or revenue requirements.

- **Transport**

Identify transport requirements (for example fleet requirements, vehicle hire, vehicle parking requirements).

- **Other service and assets**

Identify any other key factors required to support the normal operations of the critical business function (for example *couriers, chemical supplies, inventory*).

Once the normal day-to-day resource requirements have been determined, managers should be challenged to identify which resources are ***absolutely*** essential to achieve the level of operation that will meet the critical business objectives in the event of a disruption. The aim here is to identify the ***minimum resourcing*** that must be made available following a disruption. The primary outcome of this step should produce two lists for each critical business function: 'normal resource requirements' and 'disrupted resource requirements'.

4.5 Step 4: Establish interdependencies

A range of interdependencies will usually need to be identified and mapped, both internally and externally. The following types of interdependency need to be considered:

- Between individual critical business functions within the organisation;

- With key suppliers (including critical infrastructure suppliers such as water, power and telecommunications utilities);
- With key customers;
- With strategic partners;
- With competitors;
- With regulators; and
- Parties where no current interdependency exists, but could be created following a disruption.

For each of these interdependencies, mapping should include details on: the nature and level of the interdependency; any critical failure points; contractual conditions; service level agreements, and so on.

A common shortcoming of many attempts at mapping interdependencies is neglecting to ensure that people and resources are mapped against business needs for a minimal level of operation.

Key contact details should be gathered while examining interdependencies. Contact details for the following stakeholders should be recorded:

- Key staff required for the operation of each critical business function;
- Key contacts for internal interdependencies;
- Key contacts for external interdependencies, including major customers, critical suppliers, regulators, etc.

Wherever practical, the following contact details should be collected:

- Business hours telephone numbers (landline and/or mobile – cell);
- After hours phone numbers (landline and/or mobile – cell);
- Fax numbers;
- Email addresses (document these – even for internal staff – as the name on the email address may be different to what the person is called commonly); and
- Contact addresses (local map references can also be of assistance).

4.6 Step 5: Determine the disruption impacts

The aim of this step is to determine the impact of each of the validated disruption scenarios upon each of the critical business functions. A variety of metrics can be employed to examine impact, however, using measurement scales similar to those used for measuring consequence during the risk assessment can be advantageous. This would build upon existing familiarity of the tool and reduce workload as the existing consequence information can be an important input to the estimation of the disruption of the impact. Both financial and operational (non-financial) measures of impact can be made (see Tables 8 and 9). Examples of different types of impact are provided in Table 10.

Table 8
Measuring financial impacts of a disruption scenario (example only)

Rating	Category	Description
1	Insignificant	Financial loss <1% budget
2	Minor	Financial loss 1-5% budget
3	Moderate	Financial loss 5-25% budget
4	Major	Financial loss 25-30% budget
5	Catastrophic	Financial loss >30% budget

Table 9
Measuring operational (non-financial) impacts of a disruption scenario (example only)

Rating	Category	Description
1	**Insignificant**	No measurable operational impact to the business.
2	**Minor**	Minor degradation of service, impact limited to a single area of the business, management intervention required.
3	**Moderate**	Substantial degradation of service, impact to multiple areas of the business, can be managed with substantial management intervention and possible outside assistance.
4	**Major**	Significant degradation of service, impact to multiple areas of the business, threatens the viability of the enterprise, and requires significant mobilisation of resources and significant management intervention including external assistance.
5	**Catastrophic**	Threatens the immediate viability of the enterprise and introduces significant long term doubt on the viability of the enterprise. Immediate action required to minimise or mitigate the effect on most parts of the enterprise.

Table 10
Examples of disruption impacts*

Class of impact	Area of impact
Financial impacts	Opportunity cost.
	Increased trading/operating costs.
	Loss of revenue.
	Losses due to physical damage or injuries.
	Capital value and depreciation.
	Increased expenses during the recovery period.
	Increased expense of backlog management.
	Contract penalties.
Non-financial impacts	Corporate reputation and brand.
	Adverse publicity.
	Legal, contractual or regulatory liabilities.
	Delivery standards.
	Intellectual property, knowledge and data.
	Political interest and comment.
	Regulatory attention.
	Stakeholder confidence and goodwill.
	Staff morale and wellbeing.
	Management control and capability.

In circumstances where the scenario could cause an increasing degradation of resources and/or capability over a period of time, it is useful to determine potential impact changes over a set period of time. For example:

Determine the impacts on critical business function x after:

- less than one hour following the event;
- one to four hours (half day) following the event;
- one day following the event;
- two to seven days following the event;
- one to four weeks following the event; and
- greater than one month following the event;

---

* Source = *Standards Australia/New Zealand Business Continuity Management, HB 221: 2004.*

4.7 Step 6: Identify the maximum acceptable outage times and recovery objectives

Maximum acceptable outage (MAO) times should be determined for each of the critical business functions (down to process level where applicable), key IT applications and other critical assets. The MAO time represents the maximum period of time that an organisation can ***tolerate*** the loss of capability of a critical business function, process, asset, or IT application. Note that this should be determined by the *'owners'* of the critical business function.

Associated with the MAO time is the recovery time objective (RTO). A RTO represents the required level of capability that the organisation ***aims*** to recover within a defined time frame. This is often determined by the *'provider'* of the infrastructure or service. Examples of recovery objectives include:

RTO 1: All Gold mainframe applications to be recovered within 12 hours of a loss incident.

RTO 2: Customer call centre to achieve 70% capability within 24 hours of a loss incident.

RTO 3: 100% of meals delivery capability to be in place within 90 minutes of a loss incident.

It is a common misconception that the business's MAO time and the IT systems' RTO should be equivalent time frames. However, there may be commonly a significant difference between MAO times and RTOs. For example:

The MAO time for processing cheque payments may be set at 24 hours (determined by the business in consultation with representative stakeholders).

The RTO is set at 72 hours by the IT provider (representing the minimum feasible time that systems can be recovered at a new site).

Such a 48 hour gap in availability means that the business must:

- Have in place existing workarounds that will provide an acceptable level of continuity for this 48 hour gap;
- Develop plans and capability for alternate manual operations to cover the 48hr gap; and/or
- Decide if the investment required to further reduce the RTO (for example by establishing a new hot site) is offset by the gains made in having a faster recovery time.

The critical success factors (identified at the start of the BIA) provide useful guidance in establishing the recovery time objectives. However, the level of capability/service defined by a RTO may also be materially different to capability/service levels defined by these critical success factors.

MAOs and RTOs can be used to prioritise the criticality and the order in which critical business functions (or critical assets, etc) will be recovered or allocated essential resources. One approach to this involves establishing a triage framework of recovery time objectives (Table 11).

Table 11
Example of a triage framework based on recovery objectives

Triage level	Criteria
Gold	Recovery back to an acceptable level within 24 hours
Silver	Recovery back to an acceptable level within 48 hours
Bronze	Recovery back to an acceptable level within 5 days

A range of other criteria can be used in the construction of a triage framework for prioritisation (see Appendix F) including:

- Contribution to critical business objectives;
- Level of risk associated with loss of the function or process;
- Time sensitivities of key success factors;
- Time deliverables in service level agreements, contracts, and similar items.

A third concept that needs to be considered is the recovery point objective (RPO). The RPO represents the time by which the organisation aims to have managed and recovered its systems and data - this often encompasses the time taken to reduce any work backlogs to acceptable operating levels. The relationship between the MAO, RTO and RPO is summarised in Figure 13.

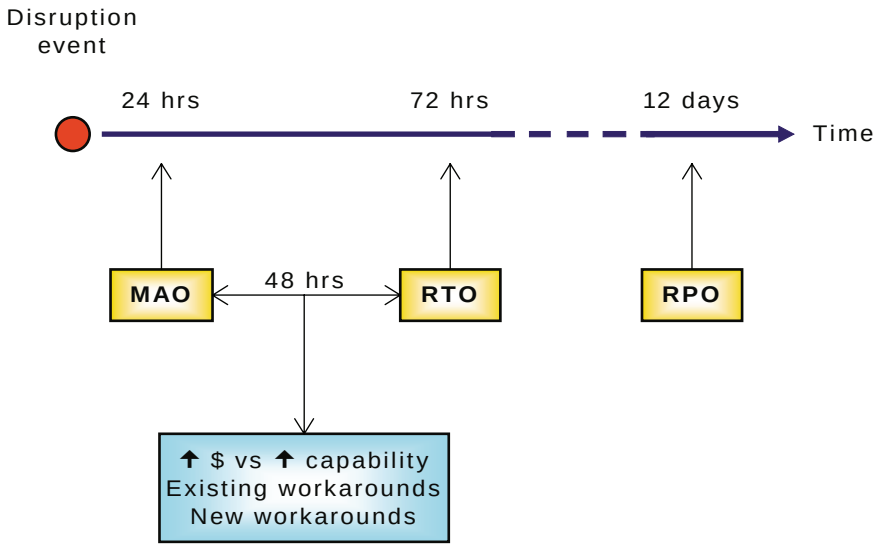


FIGURE 13 RELATIONSHIPS OF CONTINUITY AND RECOVERY OBJECTIVES (EXAMPLE ONLY)

4.8 Step 7: Identify alternate workarounds and processes

There will be circumstances when the available capability is not sufficient to maintain processes and critical business functions, or when the delay before recovery occurs is not acceptable. At such times the only means available to continue the achievement of critical objectives is to implement alternate workarounds. The commonest approach to alternate workarounds is the use of manual processes to replace the non-available automated processes. For example, a simple alternate workaround for the loss of a word processing application may be the use of pen and paper for document preparation.

The starting point for the identification of alternate workarounds should be the creation (if not already available) and examination of process maps in order to:

- Review the appropriateness of the existing process from both an efficiency and effectiveness perspective;
- Determine any redundancies within the existing processes; and
- Examine the potential for process change and improvement, rationalisation, adoption of different processes, replacement of automated processes with manual procedures, or other mechanisms for achieving the process outputs or outcomes.

Criteria to consider in identifying and evaluating alternate workarounds include the degree to which:

- The alternate process can be conducted in the absence of technology or specialised equipment in the event it is not accessible;
- The alternate process can be practically implemented following a disruption;
- The alternate process will produce outputs that meet a minimum acceptable standard;
- Significant OHS issues arising as a result of the adoption of the alternate process can be effectively managed;
- Sufficient knowledge and skills can be accessed to manage and operate the alternate process; and
- The alternate process will comply with any governance, regulatory or contractual requirements.

4.9 Confirming current preparedness

The final step involves confirming the current preparedness of the critical business function(s) to continue to operate during a disruption. This involves confirming that appropriate resources and workarounds are appropriate to manage the agreed outage times and that the relationships with interdependencies can be managed. In determining the current preparedness reference should be made to the analysis of control effectiveness and vulnerability conducted during the risk assessment (Chapter 3). This should also include the identification, recording and evaluation of existing business continuity and disaster recovery plans.

Issues that should be considered in determining the current preparedness include:

- **Equipment redundancy**

Similar equipment used in different parts of the business, alternate external sources for equipment, lease arrangements, etc.

- **IT systems redundancy**

Similar multiple networks at different locations, transportability between networks, existence of hot sites, warm sites and cold sites, etc.

- **People**

Availability of trained specialists, multi-skilling, contractor availability.

- **Facilities**

Availability of alternate accommodation, presence of suitable infrastructure (eg data cabling), etc.

- **Communications**

Arrangements for emergency/disruption communications eg public websites, confidential staff information websites, arrangements with media providers, etc.

- **Data**

Resilience of security systems, back-up systems, off-site storage arrangements, etc.

- **Paper records**

Alternate access arrangements, multiple copies, secure storage, electronic copies.

- **Suppliers**

Existence of multiple suppliers, supplier's own continuity arrangements (particularly sole suppliers), etc.

- **Assistance**

Types of external assistance available, for example arrangements with competitors (eg for customer assistance, inventory sharing, etc), contractor and lease agreements, 3rd party access, etc.

NOTE: The effectiveness of many of these preparedness measures will already have been examined during the vulnerability analysis.

4.10 Summary

- The business impact assessment provides information on the effects of identified risks (or risk scenarios) on critical business functions, critical infrastructure or the organisation as a whole.
- The assessment provides for a prioritisation of BCM activities and associated implementation resources.
- The assessment identifies areas where improvement is required to better protect the organisation from the consequences of disruption risks.
- Outcomes from the BIA include the identification of:
  - critical organisational objectives and performance levels that must continue to be achieved following a disruption,
  - key personnel essential for conducting any required response to a disruption,
  - normal operational resource requirements and minimum resource requirements during a disruption,
  - critical interdependencies between each critical business function and other internal and external third parties,
  - areas requiring alternate workarounds, and processes or activities that cannot proceed, and
  - contact details for key stakeholders, including employees, customer and suppliers.

To assist in the implementation of the *Business Impact Assessment* step, a checklist is provided at Section 4.11 and templates for information gathering at Section 4.12.

4.11 The BIA checklist

Element	Issue	Activity status: Not started	Delayed	On target	Completed	Comments
Communications	Has a BIA communications approach been developed and implemented?					
	Have disruption scenarios been modified and/or confirmed with 'owners' of critical business functions?					
Critical business functions	Have critical business functions been identified and confirmed by the 'owners' within the business?					
	Have key processes and sub-processes been identified?					
	Have key success factors been identified for each critical business function?					
	Have critical business functions been prioritised for post-disruption resumption?					
Resources	Have current (normal) resourcing requirements been identified?					
	Have resources required during a disruption been determined?					
Interdependencies	Have interdependencies for each critical business function been identified?					
	Have both internal and external interdependencies been considered?					
	Have both downstream and upstream interdependencies been identified?					
	Have contact details been confirmed?					

Element	Issue	Activity status: Not started	Activity status: Delayed	Activity status: On target	Activity status: Completed	Comments
Disruption Impacts	Have the impacts of disruption been determined for each critical business function?					
	Have a range of financial and non-financial impacts been assessed?					
	Have MAO times and RTO been determined for each critical business functions?					
Preparedness	Has current preparedness and capability been assessed?					
	Have treatments been developed to address preparedness and capability gaps?					
	Have alternate processes and workarounds been identified?					
	Are resources and skills available to implement workarounds?					

4.12 BIA templates

Identify periods of high (H), medium (M), and low activity on a seasonal, monthly or weekly basis

Identify the key contact for each critical business function (also record the name of the person who provided the information - if different)

Template 4.1
Workload demand and variation

Critical business function	Critical dates																			Specific priority dates	Key contact person
	Month												Days								
	J	F	M	A	M	J	J	A	S	O	N	D	M	T	W	T	F	S	S		
Regional sales	L	M	M	M	H	H	H	H	H	H	H	L	H	M	M	M	H	L	L	Last Friday of each month	Ivor Dheel

Identify each critical business function

Identify specific dates in the calendar when predictable periods of high activity are likely to occur

Template 4.2
Determining impacts on the business

Determine the non-financial impacts of a disruption for each period

Identify the time within which full recovery (for example including processing backlogs) will be completed

Identify each critical business function

Record the maximum acceptable period of time for loss of capability

Critical business function	Impacts												Highest Impact *(Provide a description of the highest rated impact)*	MAO *(Maximum acceptable outage)*	RTO *(Recovery timeframe objective)*	RPO *(Backlog processing)*
	Financial impacts *(rate 1 to 5)*						Non-financial Impacts *(rate 1 to 5)*									
	<1 Hour	1 -4 Hours	1 Day	2 - 7 Days	1 - 4 Weeks	> 1 month	<1 Hour	1 -4 Hours	1 Day	2 - 7 Days	1 - 4 Weeks	> 1 month				
Accounts payable	1	1	1	1	2	3	1	1	1	1	3	4	Significant reputational harm and loss of supplier confidence after 30 days	30 days	14 days	40 days

Determine the financial impacts of a disruption for each period

Describe the nature of the highest recorded impact

Identify the intended time to recovery of minimum acceptable capability (eg restore IT systems)

Record the Critical Business function identified previously

Identify minimum resourcing requirements for each time period following a disruption

Template 4.3
Determining resource requirements

Minimum resource requirements								
Critical business function/process: invoice processing								
Resources	**Current resource level** *(available to complete key business process)*	**Resource requirements** *(Minimum levels required to complete key business process)*						**Manual alternate workarounds** *(Yes/ No)*
		<1 hour	**1 to 4 hours**	**1 Day**	**2 to 7 Days**	**1 to 4 weeks**	**> than 1 month**	
Staff	1 manager 8 staff	**1 mgr** **1 staff**	**1 mgr** **1 staff**	**1 mgr** **1 staff**	**1 mgr** **1 staff**	**1 mgr** **4 staff**	**1 mgr** **6 staff**	N/A
IT applications	SAP Oracle	Nil	Nil	Nil	SAP Oracle	SAP Oracle	SAP Oracle	Yes
Telephones	9	1	1	2	2	3	4	Yes

Identify each type of resource required

Record current resourcing levels

Determine if manual workarounds or other alternate solutions are available

Record the Critical Business function identified previously

Identify alternate member of staff with the competencies to fill this position if required

Identify the key positions required in the event of a disruption

Template 4.4

Determining responsibilities and operational activities

Critical business function: issues management				
Person	**Position**	**Alternate or standby**	**Key responsibility/activity**	**Reports to**
Don Penik Ext 6060	Manager, Issues Management	Ed Le Schikan (Snr Account Executive)	Oversight of function Coordinate response Approve media releases Brief Chief Executive Brief crisis Management Team	D.R Spinn Director Public Affairs
Ed Le Schikan Ext 9999	Snr Account Executive	Hardly Hier (Account Executive)	Prepare response Coordinate and collate information Prepare media releases Arrange briefing sessions	Don Penik Manager Issues Management

Identify the key people required in the event of a disruption

Identify the key positions required in the event of a disruption

Identify the key activities that can be undertaken in the event of a disruption

Identify the specific critical business function

Identify any significant workarounds that can be employed

Template 4.5
Determining alternate workarounds

Critical business function: market analysis			
Critical resource requirement	**What critical tasks/activities/processes <u>can</u> be performed**	**What critical tasks/activities/processes <u>cannot</u> be performed**	**What alternative processes or workarounds can be employed**
Personal computer Standard operating environment MarkAT (market analysis application)	Analysis of available data (hard copy) Liaison with other agencies Completion of initial analysis	Personal electronic data file will not be accessible Internet based information will not be accessible Correctly formatted reports will not be developed Email will not be accessible Analysis will not be a s comprehensive as would otherwise be the case	Reports can be handwritten Phone fax and post can be used to provide and distribute information Increased time requirements to complete reports - therefore lower priority tasks cannot be undertaken

Determine critical resource requirements (refer to Template 4.3)

Identify what can still proceed in the total absence of the required infrastructure

Identify what cannot still proceed in the total absence of the required infrastructure

Identify major internal and external customers and stakeholders

Identify alternate arrangements which can be undertaken if the normal operation is disrupted

Template 4.6
Determining customer dependencies

Critical business function	Major customer/stakeholder	Key contacts – details	Minimum contracted or acceptable requirements	Alternate continuity arrangements
Security threat assessment	Internal: Senior executive management	Ima Skerd Snr Executive PA to the CEO L 6 Curzon House Tel no: 03 9123 4567 Fax no: 03 9123 7654 Mobile no 0401234567 Alternate contact: Shesa Chékan Executive Reception L 6 Curzon House Tel no: 03 9123 4568 Fax no: 03 9123 7658 Mobile no 0401234566	Weekly review of key global threats Emerging threats identified and assessments delivered within 48 hours Initial response to request within 4 hours	Work can be conducted at any location where internet and telephone access is provided Alternate: general assessments can be obtained from: Randy Sway, Central Security Coordination Office Tel: 02 1234567 Fax: 02 1234566 Email: sneaky@secret.gov.au

Determine critical business functions

Identify contact details for major customers/stakeholders

Identify customer's minimum acceptable requirements – contracted or otherwise

Identify supply requirements to meet the minimum acceptable level of performance (refer to Template 4.3)

Identify all internal and external suppliers of critical goods and services

Template 4.7
Determine supplier dependencies

Critical business function: security threat assessment			
Contracted goods and services	**Minimum acceptable goods and services**	**Supplier contact details**	**Alternate supplier contact details**
Intelligence briefings and reports on request Contract requirements specified at purchase request	Domestic intelligence update within 24 hours International intelligence updates within 48 hours	Jim Blofeld, Spectre Consulting Mobile: 0408 666666	Penny Monet, Bonded Services Mobile: 0408 101010 Requires 24 hours notice for work up

Identify what the supplier is expected or required to supply. The existence and location of formal contracts should be detailed

Provide information on possible relevant alternate suppliers, including any restrictions on their use

5 Developing BCM Strategies—Reaction to an incident

The development of BCM strategies is concerned with determining how an organisation will react to an incident, and the manner in which the different elements of this overall response will interact. Typically an organisation responds to an incident in three broad phases:

- The emergency response (this equates to the '*Response*' component of *PPRR* in emergency management*);
- The continuity phase; and
- The recovery phase†.

Activation of these phases would normally be expected to occur in a sequential order however, there can be significant overlap in the duration. Furthermore, depending upon the circumstances, the time between activation of the individual response could range from seconds to weeks (Figure 14). In some situations, a phase may not in practice even be activated. For example where there is no threat to life or property following an incident, the emergency response may solely consist of an assessment and decision that activation of such a response is not required.

In the development of any strategies for these phases there are a number of issues that must be considered:

---

* PPRR: Preparedness, Prevention, Response and Recovery comprising the Comprehensive Approach in emergency management; in Emergency Management Australia. (1993). Commonwealth counter disaster concepts and principles. Canberra: Emergency Management Australia.

† Both the continuity and recovery phases equate to 'Recovery' as used in the PPRR framework.

- Regulatory, policy or industry standards requirements that must be addressed;
- Availability and suitability of alternate strategies;
- Costs and benefits of strategy options;
- Collateral or additional risks created by different options; and
- Organisational capability to implement strategies.

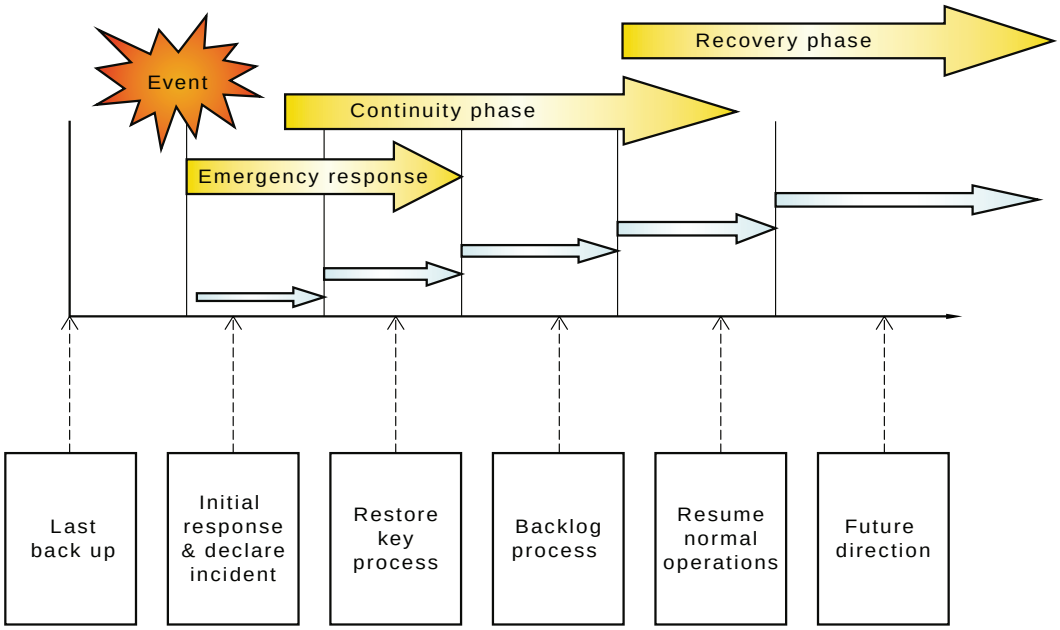


FIGURE 14 THE THREE PHASES OF MANAGING A DISRUPTION

5.1 The emergency response

The emergency response is the immediate response to the event. It is primarily concerned with the protection and preservation of life and property. The emergency response could be as simple as the activation of a building evacuation plan, or as comprehensive as an emergency management strategy involving the immediate protection of property, people and information across multiple sites or communities.

Typically the development of the emergency response strategy will involve:

- Determining regulatory and industry standards' requirements (eg for fire evacuation);
- Determining organisational objectives and requirements for the emergency response;
- Confirming existing emergency response plans and capabilities;
- Identifying gaps that require further development;
- Identifying triggers for the activation of plans;

- Identifying responsibilities for components of the response strategy/plan;
- Documenting the strategy including the identity and location of component plans; and
- Identifying command, coordination and control requirements for the response, including any approaches to ICS* or EOCs† that may be needed.

5.2 The continuity phase

The main purpose of the continuity phase is to ensure the continued delivery of a minimum acceptable level of performance. The important considerations in developing the strategy for this phase are:

- Confirming the objectives for continuity as previously identified through the *Commencement* and *BIA* steps;
- Determining the level that detailed continuity plans need to be developed to. For example are plans required for:
  - critical business functions?
  - key processes?
  - specific assets, facilities, locations, or other infrastructure?
  - key people?
  - key supply relationships?
- Determining the structure of continuity planning documents that need to be produced. For example:
  - will one plan or multiple plans be developed?
  - will plans be developed in a hierarchy with consolidated departmental level plans sitting above local functional plans?
- The format, level of detail and content requirements for plans;
- Confirming that the identified critical business functions (or assets, facilities, etc) are still appropriate. This may lead to the consolidation of one or more business functions into a single critical business function for planning purposes in order to improve the efficiency and effectiveness of subsequently developed plans. Alternatively it may become apparent that planning for one or more identified critical business functions is no longer required to achieve the stated objectives;
- Identifying criteria for activating the continuity phase (i.e. triggers); and

---

* ICS = incident command system

† EOCs = emergency operations centres

- Identifying criteria of the deactivation, step down, or stand down of the phase.

5.3 Recovery and restoration phase

The recovery and restoration phase is aimed at returning the organisation to a long-term operationally acceptable and sustainable capability. In developing a recovery and restoration strategy it will be necessary to consider what can be practically identified and planned for and what will be decided on following the actual incident. This will involve identifying issues that are either event-independent or event-dependent. Many activities that may be required during recovery are highly event-dependent, for example there are very specific issues to address in recovering from a catastrophic building fire (for example seeking new permanent premises, arranging for rebuilding renovation) compared to a localised fire in IT's server room (for example purchase or lease of new equipment, evaluation and installation of new fire suppression systems). There will be limitations as to what pre-incident planning can be undertaken for event-dependent issues.

Issues to consider in determining the strategic requirements of the recovery and restoration phase include:

- **What are the key recovery and restoration objectives?**

For example return to pre-event capability, implementing process improvement/re-engineering initiatives, etc.

- **Who will be members of the recovery team?**

Again this will in many circumstances be very event-dependent.

- **How will environmental scanning be undertaken?**

It will be vital to have a thorough understanding of changes to the external and internal environments following the event in order to inform decision making on the recovery of the organisation.

- **How will performance be monitored and reported?**

The recovery team need to be fully aware of current capability and performance and how these factors are changing in phase to their recovery efforts.

- **What are the priorities for residual backlog management?**

The management of backlogs should have been a key consideration during the continuity phase. However, as the business is returned to 'normal' capability there is likely to be a continuing backlog of work that still requires attention.

- **What decision-making processes need to be established to consider investment/divestment issues?**

These could be at the simple level of disposal, repair or replacement of plant or other assets, or could involve more strategic considerations such as mergers, acquisitions, strategic alliances, entry into new markets or withdrawal from existing markets.

- **If documents or electronic media are damaged what are the restoration priorities?**

Following a fire or flood there may be significant quantities of damaged documents or other media. The ability to restore these items may be severely hindered by time (urgency) or financial constraints. How documents and electronic media will be prioritised for restoration should be considered as a key element of planning (see Appendix F for an example triage system).

- **What are the requirements for insurance claims management?**

Decisions need to be made regarding the coverage required for business disruption insurance, for example should cover extend: to loss of revenue, costs of re-establishing premises, removal to alternate sites, replacement of key infrastructure, etc.

5.4 Summary

Strategies are required for the:

- **Emergency response**

The immediate reaction to a disruption focusing on the protection and preservation of life and property.

- **Continuity phase**

Focusing on establishing a minimum acceptable level of capability and performance.

- **Recovery phase**

Focusing on returning to a routine operational capability and performance.

Strategies need to focus on:

- Meeting regulatory, industry and organisational requirements.
- Providing appropriate cost–benefit returns.
- Matching strategic objectives with the practical realities of access to capabilities and resources.

To assist in the implementation of the *Developing BCM Strategies* step, a checklist is provided at Section 5.5 and templates for information gathering at Section 5.6.

5.5 The strategy development checklist

Element	Issue	Activity status: Not started	Delayed	On target	Completed	Comments
Emergency response	Have objectives been developed for the emergency response?					
	Has a clear understanding been developed of regulatory and industry standards requirements for the emergency response?					
	Have existing emergency response plans been reviewed?					
	Have strategy options been developed for the emergency response?					
	Has a cost–benefit analysis been conducted as part of the selection of the recommended options?					
	Have activation and deactivation criteria been developed for the emergency response?					
	Have incident control and coordination requirements been developed and planned for?					
	Have preparatory activities been identified for the emergency response?					
Continuity phase	Have objectives been developed for the continuity phase?					
	Has a clear understanding been developed of regulatory and industry standards requirements for the continuity phase?					
	Have existing continuity plans been reviewed?					
	Have strategy options been developed for the continuity phase?					
	Has a cost–benefit analysis been conducted as part of the selection of the recommended options?					
	Has a plan and process been developed for undertaking environmental scanning during the disruption?					

		Activity status				
Element	**Issue**	**Not started**	**Delayed**	**On target**	**Completed**	**Comments**
	Have activation and deactivation criteria been developed for the continuity plans?					
	Where multiple continuity plans exist have coordination requirements been developed and planned for?					
	Have preparatory activities been identified for the continuity phase?					
Recovery and restoration phase	Have objectives been developed for the recovery and restoration phase?					
	Have existing recovery and restoration plans been reviewed?					
	Have strategy options been developed for the recovery and restoration phase?					
	Has a cost–benefit analysis been conducted as part of the selection of the recommended options?					
	Have activation and deactivation criteria been developed for the recovery and restoration phase?					
	Have coordination arrangements with the emergency response and continuity phase been developed and planned for?					
	Have preparatory activities been identified for the recovery and restoration phase?					
	Has a process been established for undertaking environmental scanning during the disruption?					
	Have priorities been identified for the management of backlogs?					
	Has a process been established to allow performance monitoring during the recovery and restoration phase?					
	Have key documents been identified and prioritised?					
	Has a strategy been developed for insurance and claims management?					

5.6 Strategy development template

Template 5.1
Strategy development

Organisational unit:	Finance Department
Location:	Level 35 Curzon House
Contact name:	Steve Idore
Title:	Supervisor
Telephone:	91234 5678
Email:	rea.locatte@finman.org

Critical business function	Cheque processing		
Critical infrastructure	Financial systems and cheque printer		
Risk scenario	Loss of access to building		
MAO time	24 hours	**RTO**	72 hours
Response requirements	Establish alternate cheque printing capability to cover 48 hour period before recovery		
Response option 1	Purchase 2nd cheque printing equipment for recovery site	**CBA*:**	Not favourable
Response option 2	Remove to bureau service	**CBA:**	Favourable
Response option 3		**CBA:**	
Response option 4		**CBA:**	
Recommended option	Remove to bureau service	**Response objectives**	Resume cheque printing to 80% capability within 24 hours
Detailed description of response	• Notification of bureau • Flat file transfer from data centre to bureau • Bureau processing of file • Verification and validation by accounts officer • Authorisation to process • Cheque collection and distribution		
Preparatory requirements			**Responsibility**
	• Develop list and contact details for approved bureaux		Steve Idore
	• Establish capability for file generation and transfer		Ricky Tee
	• Develop alternate verification and validation process		Ricky Tee
	• Develop alternatives for cheque collection and distribution		Steve Idore

Develop options to address the response requirements

Undertake a cost–benefit analysis for each option (qualitative and/or quantitative)

Describe the key components of the recommended response option

Identify actions that have to be undertaken before plans are completed

Identify responsible individuals for each preparatory action

* CBA – Cost–Benefit Analysis

6 Assessing and collating resources requirements—Consolidating resource information

Once strategies have been developed, resource requirements need to be confirmed as appropriate to achieving these strategies. The identification of resources previously conducted in the *BIA* (see *Chapter 5*) focused on the needs of individual critical business functions. This next stage involves collating information from across multiple critical business functions for subsequent planning purposes. In particular the need is to ensure that synergies and conflicts in resource availability, access and use are identified and managed.

Key types of resources that should be considered in consolidating requirements are summarised in Table 12. There are a number of factors that need to be considered at this stage:

- Type and volume/quantity of resources required for each process during the disruption;
- Current location or source for each resource identified above;
- Dedicated resource requirements, i.e. processes or locations that require the named resources to be dedicated to their use (in their entirety or in part);
- Access requirements, where processes or locations require access to the use of resource, but do not require dedicated resources;
- Identification of synergies between processes/locations in the use or application of resources; and
- Identification of conflicts between processes/locations in the use or application of resources.

One approach to consolidating and summarising this information is to construct a resource matrix (see Appendix G) that allows for the mapping of requirements and availability across the whole or parts of an organisation. This is also a useful way of readily identifying any conflicts in resourcing demands or allocation.

Consolidation of resource information needs to consider both internal and external interdependencies. There can be particular advantages for establishing single points of contact within the organisation for each of these interdependencies (for example improved efficiency and effectiveness in communications, logistics, purchasing, etc).

Consideration needs to be given to consolidating information on relationships with:

- Clients and customers;
- Suppliers;
- Strategic partners;
- Contractors; and
- Competitors.

During this consolidation access to other sources of information should be documented, including:

- Contracts;
- Service level agreements;
- Compliance requirements;
- Warranties; and
- Third party continuity documentation.

Table 12
Consolidation of resource information

Resource	Consolidation issues
Vital records (hardcopy and electronic)	• Identity of key prioritised documents (eg using a triage system). • Location of documents. • Special storage requirements. • Offsite storage arrangements. • Recovery time for availability. • Required frequency of access. • Records recovery and restoration procedures and suppliers.
Staff	• Critical personnel by function and location. • Identification of individuals with multiple/conflicting responsibilities. • Contact lists and call out trees. • Directory/listing of specialist expertise.
Management	• Responsibilities, accountabilities and delegations, eg for: – Critical business functions, – Sites/facilities, – Release of emergency budget/special funds, – Activation and deactivation of plans.
Process information	• Identification and location of standard operating procedures (SOPs), operating manuals, etc.
Accommodation and facilities	• Current facilities use (eg using matrix). • Post disruption facilities requirements (eg using matrix). • Accessibility/availability/conflict with specific facilities. • Location of accommodation/facility maps. • Map references/ street guides to alternate accommodation. • Accommodation (eg switchboard) phone numbers for current and alternate sites. • Office, plant and other specialist equipment requirements.
IT infrastructure and applications	• Dependencies on infrastructure and application mapped against each critical business function/ location. • Minimum acceptable outage times documented.
Telecommunications	• Requirements for dedicated versus access only availability of telecommunications equipment. • Identification and location of equipment ‘surplus’ to requirements, post disruption (eg mobile phones held by non-essential personnel).
Utilities	• Utility requirements by location. • Alternates to normal supply of utilities (eg backup generators, water tanks, etc), operational requirements, manuals, locations, identification of individuals skilled in their use, etc.

6.1 Assessing organisational capabilities

Analysis is now required to determine to what extent current capability can address the potential impacts of future disruptions and deliver the identified strategies. Issues to consider in this analysis are summarised in Table 13, and comprise information that needs to be included in the BCP, pre-event preparation and in business improvement.

Table 13
Assessing organisational capabilities

Issue	Current capability*	Future capability
Process capability	Resilience and flexibility to continue operation during a disruption.	Feasibility and availability of alternate workarounds.
Personnel capability	Skilled and trained individuals identified capable of fulfilling process responsibilities during a disruption.	Individuals familiar with and capable of undertaking alternate workarounds.
Resource capability	Availability of and access to existing resources during a period of disruption. Adequacy of these resources to supporting process requirements.	Availability or access to any additional resources required from third parties. Need for agreements in principle, etc for supply of these resources.
Command and control	Existing authorities, delegations, accountabilities and responsibilities.	Access to approval and accountability systems post disruption. Need for the appointment of approved deputies. Knowledge and capability of individuals to fulfil deputised roles.
Interdependencies	Current interdependencies, including synergies and conflicts in resource access and use.	Changes to these interdependencies post disruption event.

6.2 Summary

- The appropriateness of identified resources needs to be confirmed against the developed strategies.
- Current and disrupted resource requirements should be consolidated from all individual plans.
- Consolidated resource maps should be reviewed to determine both ‘spare capacity’ and resource conflicts in the event of a disruption.

---

* Both current and future capability should be assessed against each of the disruption scenarios identified.

The organisational capabilities need to be assessed to ensure that the impacts of disruptions can be addressed and the identified strategies delivered.

To assist in the implementation of the *Assessing and Collating Resource Requirements* step, a checklist is provided at Section 6.3.

6.3 The assessing and collating resources checklist

		Activity status				
Element	**Issue**	**Not started**	**Delayed**	**On target**	**Completed**	**Comments**
Consolidating resource information	Has information on common resources been collated and consolidated?					
	Have synergies and conflicts in resource availability and allocation been identified and resolved?					
Assessing organisational capabilities	Has process capability been assessed?					
	Has personnel capability been assessed?					
	Has resource capability been assessed?					
	Has the capability of command and control arrangements been assessed?					
	Have the interdependencies been assessed?					

7 Writing the Plan—Guiding principles

One of the most important issues in writing a plan for managing a disruption is to ensure that it is written so that it can be understood and applied by those expected to use it. A plan should be written in such a way that it could be understood by someone who has not previously seen the document. For certain functions it is possible that the plan may have to be activated and operated by individuals not fully familiar with the processes and procedures being employed. The key issues in writing such plans include the following:

- **Simplicity**

Avoid complex and convoluted instructions – use easy to understand and easy to follow steps.

- **Language**

Wherever practicable write with the layperson in mind, not the technical specialist. Avoid using acronyms and slang – they may mean something very different to different readers of the plan. If there are different languages spoken within the workplace, to what extent do the plans need to reflect this?

- **Assumptions**

Don't assume that the reader will innately know key requirements. If it is important - document it. Don't ignore the inclusion of important information just because it is an obvious issue. It may not be so obvious to other parties.

- **Clarity**

Provide information in a format that can be readily understood. Take care in drafting the plan and test its readability with parties not familiar with the area covered by the plan.

- **Flexibility**

The plan may be required in response to one of many different scenarios. Wherever practicable try to avoid writing from the perspective of an isolated or limiting scenario.

- **Comprehensive**

Provide sufficient detail in the plan to make it a useable document that will inform and direct actions following a disruption event.

- **Brevity**

Avoid creating lengthy volumes that will be onerous, difficult to read, hard to comprehend, and are too wordy to be easily followed when activated.

- **Achievable**

The requirements detailed in the plan must be achievable in the circumstances likely to be prevailing when the plan is deployed. A plan that requires a level of capability difficult to attain in normal operations, may never reach that required capability following a disruption event.

- **Complementarity**

Plans must be complementary to other plans. Care must be taken to ensure that plans do not promote an unreasonable competition for scare resources.

- **Confidentiality**

Plans may need to be accessed by a number of individuals, attention needs to focus on the appropriate management of confidentiality and privacy issues.

- **Accessibility**

Plans need to be readily accessible by those required to use them. Plans should not be kept hidden and locked away until a disaster strikes. People that need to use the plans need to be able to read them. Individuals need to understand the content of plans and be confident of their appropriateness, and in their application from the time documentation starts.

7.1 The framework of plans

There is no ready answer for what framework of plans should be developed, it will very much depend upon the organisation's context and mode of operation. For example, a small business may only require one BCP to be developed to meet all of its requirements, whereas a medium to large business may require multiple plans to be developed – one for each of its critical business functions and key locations.

Where numbers of plans are required to cater for complex operations and structures, hierarchical planning structures are often employed (Figure 15), for example:

Tier 1 plans: Corporate whole of business plans providing for management of integrated organisation wide issues, including control of Tier 2.

Tier 2 plans: Business department/area or location plans providing for consolidation and management of a group of related Tier 3 plans.

Tier 3 plans: Multiple plans developed, one for each critical business function or process.

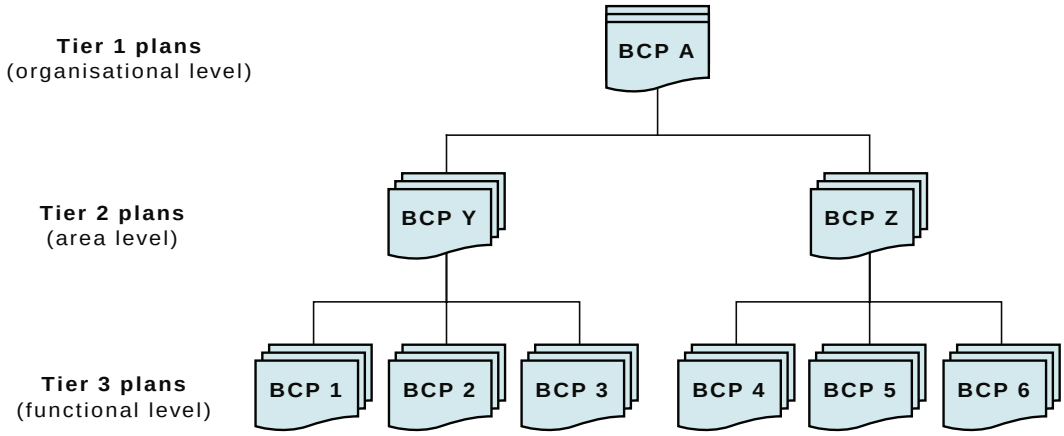


FIGURE 15 EXAMPLE OF A HIERARCHICAL FRAMEWORK OF PLANS

7.2 Content of plans: generic

The content of plans will very much depend upon the context of each individual organisation. In some circumstances regulatory requirements or industry standards will provide specific guidance on the content (for example: emergency evacuation plans). Although for the majority of plans there will be no predetermined standard, as a minimum the following generic information should be provided:

- Version control;
- Criteria for activation of the plan;
- Specific actions and responsibilities;
- Resource requirements;
- Communications requirements; and
- Contact lists.

7.3 Contents of plans: Specific

Emergency response plans

The detailed content of emergency response plans may be specified by regulations, national standards (for example fire emergency evacuation plans), or by generally accepted practices (for example industry specific or local community emergency management plans) and as such is outside of the scope of this Handbook.

Business continuity plans

The BCP's content must be developed to reflect the organisation's context and provide the required capability to support the achievement of critical objectives. A number of issues need to be considered in writing the BCP. These issues may either be included within the body of the BCP, or in other relevant documents, with their locations referenced in the BCP (see Table 14). Suggested content and structure for other plans, such as critical incident management, incident coordination plans, small organisational BCP, etc are at Appendix H.

Table 14
Recommended content for a BCP

Content	Description
1 Introduction	
1.1 Organisational details	Name of organisation, location, areas specifically covered by the plan, etc.
1.2 Objectives	Key organisational objectives that the plan is addressing.
1.3 Purpose	Specific purpose of the plan.
1.4 Critical business function	Details of the critical business function, process, critical asset, etc to which the BCP refers.
1.5 Assumptions	Key assumptions made in developing the plan, eg availability of key resources, constraints on scope of the plan etc.
1.6 Processes	Processes, subprocesses, etc that comprise the critical business function, or support the use of the asset/facility.
1.7 Activation and stand down	Events, outage times, etc, that serve as triggers for the activation and deactivation of the BCP. Arrangements, processes etc for activation and stand down.
1.8 Responsibility	Named individual(s) with responsibility for the creation and maintenance of the plan.
1.9 Version control and maintenance	Version number of the plan, date of creation, date of next review, details of reviews authorisations, sign-off of plan etc.
2 Operational requirements	
2.1 Critical success factors	What level of capability the critical business function, asset etc must achieve. Specific contractual and regulatory delivery requirements should also be specified.
2.2 Interdependencies	Key internal and external interdependencies.
2.3 Outage times	Where relevant identify minimum acceptable outage times and/or required recovery time for critical functions, processes, resources etc.
2.4 Compliance	Compliance requirements and other obligations that have to be met following activation of the plan (eg regulatory, policy, contractual obligations etc)
3 People	
3.1 Structure	Structure and reporting relationships of the team operating under the plan
3.2 Roles and responsibilities	Roles and responsibilities of named key managers and staff.

(*continued*)

Table 14 (*continued*)

Content	Description
3.3 Contact details	Business and after hours contact details of key managers, staff, supplier's customers and other stakeholders. Wherever possible each key role should also have a deputy identified and alternate suppliers listed.
4 Continuity arrangements	
4.1 Coordination	Arrangements for coordination between plans and across multiple locations.
4.2 Accommodation	Details of alternate/backup site arrangements.
4.3 Resources	Types and quantities of resources required to support the activation and implementation of the BCP. The plan should specify if dedicated resources are required or if access to shared resources is available. Include: • People • Information and documentation • Accommodation • Plant and property • Budget • Assets and other equipment • Telecommunications • IT systems and applications
4.4 Workarounds and alternate solutions:	Identify tasks that can still be undertaken following a disruption, those tasks that cannot be undertaken and alternate solutions to those tasks to still achieve acceptable outcomes.
4.5 Continuity management tasks	Identify additional activities that have to be undertaken in response to the disruption (i.e. those activities beyond those associated with routine activities), for example assessment of the impacts of the disruption, coordination of asset reallocation, staff briefings to be held, etc.
5 Communications	
5.1 Communications	Summary of communications requirements following activation of the plan
6 Appendices	
6.1 Other plans	Details of other related plans, availability, location and access.
6.2 Checklists	Activity checklists, aide memoires, etc.
6.3 Maps and drawings	Location maps, site maps, architect drawings, layouts, etc.

7.3.1 Recovery and restoration plans

Plans for the recovery and restoration of critical business functions will be even more dependent upon the context than is the case for BCPs. Therefore any specific table of content is likely to be useful to only a narrow range of scenarios and organisational requirements. However, many of the elements detailed in Table 14 can be applied to documenting a recovery and restoration plan.

7.4 Summary

- Plans should be written using the guidance principles to ensure their useability when required following a disruption.
- Plans should be developed for example, for functions, locations, infrastructure, etc according to the organisation's context and priorities.
- There is no standard content for a plan, although regulation, industry standards etc may require certain issues to be covered in the written documentation.
- An example list of contents can provide useful guidance in documenting the plan.

To assist in the implementation of the *Writing the Plan* step, a checklist is provided at Section 7.5.

7.5 The continuity plan checklist

		Activity status				
Element	**Issue**	**Not started**	**Delayed**	**On target**	**Completed**	**Comments**
Plan development	A plan(s) has been written in a manner that considers the guiding principles.					
Plan content	The content of the plan(s) considers the broad range of issues required to mount an effective response to a disruption.					
Framework	The need for multiple plans at critical business function and organisational level has been considered.					
Scope	Requirements for the plans for emergency, continuity and recovery plans have been identified.					
	Written plans have developed that address issues identified in the scope.					
Referencing	Where information resides in documents other than the plan, this information is appropriately referenced within the body of the plan.					

8 Developing the Communications Strategy

8.1 Introduction

It is vital that communications are considered as one of the highest priorities throughout all BCM activities, both pre- and post-event. There are three broad areas for which the development of communications strategies are essential:

- Informing and consulting internal and external stakeholders on the conduct of the BCM program and development of the plans (‘*process communications*’ discussed previously in Section 1);
- Provision and receipt of information relating to the management of the incident, (some times called crisis communications) including:
  - nature of the event and disruption that has occurred,
  - emergency response,
  - the organisation’s continuity activities being implemented,
  - the range of recovery and restoration activities being undertaken,
  - other post-event requirements; and
- Dialogue concerning the ongoing maintenance of developed plans (involving process communications, see Section 9).

8.2 Communication during and after incident

The first step in developing a communications strategy to support the organisation’s emergency, continuity and recovery objectives is to define the:

- **Communication objective**
  - What is the desired outcome from undertaking communications?

  For example:

  - keep staff informed of the nature of the event and its impact on the business,
  - inform key customers of the extent and possible duration of service loss;

- **Scope of the communications**

What parties are involved (eg staff, customers, regulators, suppliers, local community organisations, etc)?

What information is required by stakeholders? What information does the organisation seek to gain? What information does the organisation seek to promulgate?

What constraints exist in providing information to third parties (eg liability issues, brand protection, privacy requirements, etc)?

How will the information be provided (eg what channels will be used – email, post, meetings, etc). The impacts of disruptions on the ability to use the chosen communication channels will also have to be carefully considered.

The communications strategy should therefore detail the nature of the communication, the means of communication and the intended audiences. From this a number of individual communications plans may need to be developed addressing the requirements of specific critical business functions/assets for particular types of stakeholders. Although all communications should be based around a two-way dialogue, communication during and immediately following an event will focus predominately on providing information to affected parties. It is also important to ensure consistency in communications whenever practical. For example through establishing simple contact points through which communications in both directions are channelled (such as the organisations ‘one voice’).

8.3 Developing the written communications plan

The issues that should be considered in developing a communications plan form the acronym CABSMACA and are summarised in Table 15.

Table 15
Communications planning issues

Issue	Considerations
Content	• Information provided is: – simple, – clear, – unambiguous. • What messages can be pre-scripted or prepared prior to an event?
Audience	• Who is the intended audience for the communication? (this is the primary audience) • What other audiences could the communication reach and be of benefit to? (this is the secondary audience) • What audiences could exploit the information for their own advantage and in doing so disadvantage the organisation? (opportunistic audience)
Boundaries	• What boundaries exist that will constrain the content or intended audience? (eg legal, political, social, technical, etc.)
Sensitivities	• What sensitivities do the communications need to account for? For example: – political correctness, – empathy and caring for people's emotions (for example following loss of life), – social and community issues, etc.
Mode	• What will be the primary channels by which the communications will be promulgated? For example: – radio, – television, – journals, – person-to-person, etc.
Assumptions	• What assumptions are being made and what arrangements need to be considered regarding audiences? For example: – social and economic standing, – religious background, – cultural perspectives, – educational levels and technical capabilities.
Capability	• What organisational capability needs to be available to: – assess the situation, – assess information needs of the organisation and stakeholders, – create and distribute communications, – evaluate the effectiveness of communications?
Accessibility	• What constraints exist and what arrangements need to be made to ensure appropriate levels of accessibility to the information for: – different language groups, – readability – for example use of plain English, – access for vision impaired, etc?

8.4 Identifying stakeholders and their needs

Communication with stakeholders should be a feature at all stages of the BCM program. However, following a disruption event, there will often be a need to prioritise stakeholders as both audiences and information sources. A lack of consideration in this respect can adversely impact stakeholder relationships for a considerable time. For example, in many major disruptions and disaster, the first port of call for affected organisations' communications specialists is with the broadcast media. Often the first information that employees will receive is via a public media report. This can be even further compounded (particularly when there is a prospect of injuries or fatalities) where next-of-kin and families become informed via the media, not through direct contact by the organisation.

Although considerable preplanning can be undertaken, there will always be a number of decisions on stakeholder communications that can only be made once the nature of the event and its impacts become understood. As part of the communications plan, an initial stakeholder communications matrix can be developed, which can begin to help identify gaps between the organisation's proposed communications and actual stakeholders expectations (Table 16).

Table 16
Example of a stakeholder communications matrix

Stakeholder	Typical organisational communication delivered	Typical stakeholder communication needed
Employees	• Organisational impact of event. • Continuing operational capability. • Alternate work arrangements.	• What has happened and why it has happened? • What will happen in the immediate future? • Where is assistance available?
Families, Next-of-kin	• The extent of the event. • Names of individuals involved and their injuries. • Access to counselling services.	• Immediately: • What has happened? • Who are the staff members involved and are they safe? • What does the family do now? • Later: • How could it happen and who is to blame?
Local community	• That an event has occurred. • Immediate safety concerns for the local area.	• Immediately: • What has happened? • Is it safe? • Could it happen again in the near future? • Later: • What is the organisation doing to ensure that it does not happen again in the future?
Customers	• That an event has occurred. • Impact on service/product delivery. • Alternate delivery arrangements.	• What is the impact on product/service delivery and quality? • How long will delivery be affected for? • How adversely will contractual conditions be affected? • Will the organisation be able to continue trading into the immediate and longer terms (longer term sustainability of supply)? • What compensation will be made available? • What other alternate sources of the product/service exist? • What is the customers' relative priority/importance to the organisation?

(*continued*)

Table 16 (*continued*)

Stakeholder	Typical organisational communication delivered	Typical stakeholder communication needed
Suppliers	• That the event has occurred. • Changes in supply requirements. • Alternate arrangements for receipt of supplies. • Alternate arrangements for accounts payable.	• Changes to supply requirements. • How long will inventory be required to be held for? • Capacity for changed pricing. • Likely duration of supply impacts. • Compensation available under contractual conditions.
Shareholders	• The nature of an event. • Immediate impacts on operational capability. • Expected recovery performance.	• Severity of the event. • Immediate impacts on sales, profits, cash flow. • Financial and brand/image impacts, short term viability, etc. • Longer term impacts on organisational valuation, share price etc. • What is being done to prevent it from happening again?
Minister	• What has happened and how. • What is being done to fix it. • What are the impacts on local communities/customers and how these are being managed. • When will normal capability and capacity be restored.	• What has happened and how? • What is being done to fix it? • What are the impacts on local communities/customers and how these are being managed? • When will normal capability and capacity be restored?
Regulators	• What has happened and how. • What is being done to fix it. • What is being done to prevent it happening again.	• What has happened and how? • What is being done to fix it? • What is being done to prevent it happening again? • What is the compliance/capability/performance of other related areas?
Special interest/ activist groups	• That an event has happened.	• What has happened? • How will the ‘group’ and its interests be affected? • Who is to blame? • What action will be taken against individuals concerned?
Media	• That an event has occurred and what has happened. • That the organisation is still operational. • What measures are being put in place. • Impacts on employees and local communities	• What has happened and how? • Who was responsible? • Can it happen again? • What similar events have happened previously?

8.5 Using IRACI

A simple project management tool, IRACI, can be adapted for use in planning communications and ensuring that each stakeholder is involved in communications at an appropriate level. This IRACI tool (Tables 17a and 17b) involves determining which individuals or groups require communications and who should be involved in providing those communications.

Table 17a
The IRACI tool

Communication action	Description
Intervention	Who has sufficient authority to intervene to halt a communication or would need to become involved if issues arise following the communication (eg adverse reaction to the communication).
Responsibility	Who has the responsibility for undertaking the communications.
Accountability	Who has the accountability for the communications, including approval of content and authorisation for release.
Consult	Who needs to be consulted as part of the communications process.
Inform	Who needs to be provided with the final communication on its release.

Table 17b
Example of the use of the IRACI tool

Intervention	Responsibility	Accountability	Consult	Inform
Issue 1: Stakeholder communication regarding loss of service				
Chairman of the Board	Public relations officer	Assistant manager stakeholder communications	General managers of operational divisions	High priority stakeholder groups
Issue 2: Supplier communication regarding establishment of recovery site				
General manager corporate services	Purchasing officer	Contracts manager	Building services manager Managers of critical business functions	Suppliers Affected staff

8.6 Understanding effective communication

A comprehensive coverage of effective communication is beyond the scope of this Handbook. However, a number of communication issues that can have a profound effect on BCM are covered briefly in this section. For communication to be effective there are a number of issues that need to be considered in the way that communications are developed and delivered, and the manner in which they are received by their intended audience. These issues include:

- *Engagement* of the audience;
- *Participation* of the audience;
- Information *transfer* between parties;
- *Adequacy* of information for decision making;
- *Comprehensiveness* of information provided*;*
- *Clarity* of information provided*;*
- *Perceptions* of individual parties involved.

8.6.1 Engagement

One of the great challenges in communication is gaining the attention of the audience to actually read or listen to the message. This challenge often arises from the very basic premise of 'it can't happen to me' so the message therefore cannot be of relevance to them. One of the prime aims of the communicator is to provide information to an audience in a manner in which they will attach meaning to that information, similar to that of the communicator. To assist in this the communication must successfully move the audience from just passive receipt of the message, to active processing of the information. The audience needs to become **engaged** with the communication and communicator.

The science of engagement is a complex and ever evolving field, beyond the scope of this Handbook. However, there are three basic principles which will greatly assist in achieving successful engagement:

- **Interest**

Both the manner and format in which the communication is presented and its content must be of interest or create an interest in the intended audience. This interest may arise because:

- the subject matter directly relates to the audiences recognised needs,
- the subject matter relates to previously unrecognised (subconscious needs),
- the subject matter creates curiosity, and /or
- the channel or approach taken in presenting the communication grabs the attention of the audience (for example, it may be unusual or otherwise stands out from the normal).

- **Emotion**

A specific communication may elicit negative or positive emotional responses in an individual. A single item of information may elicit a whole spectrum of responses across the audience, so the communicator must carefully consider the emotional response they wish to elicit. It must also be recognised that the actual elicited audience response may not be aligned with this desired response. Where the desire is to create some anxiety in order to drive behavioural change (for example, smoking can damage your health), the actual response may make individuals so distressed that they begin to avoid the information being presented. The emotional response to a communication will therefore affect the way in which individuals process its content. To engage the audience, the desired emotional response and the actual triggered emotional response must align as closely as possible.

- **Understanding**

To become engaged the audience must be able to understand the information presented or be capable of gaining an understanding within the desired timeframe.

8.6.2 Participation

Effective communication also depends upon having the participation of each of the parties involved. Attaining engagement and facilitating understanding is a key aspect of gaining participation along with:

- **Need fulfilment**

Participating in the communication must be recognised as meeting the needs of the parties involved.

- **Ability, capability**

The parties involved must have the abilities and capabilities to become involved.

- **Opportunity**

The parties must be provided with and be able to recognise the opportunity to become involved.

- **Trust**

Trust must exist, or be developed, between the parties involved. This extends to trust in:

  - the source of the information,
  - integrity and validity of the information itself,
  - the recipient of the information, and
  - the way that the information will be used.

8.6.3 Information transfer

The manner in which information is transferred, ultimately, will be determined by the success of information ***push*** (dispersal or transmission of information by the communicator) and the success of the information ***pull*** (the willingness and capability to receive the information). Success in these areas is governed by both hard (technical and infrastructure) and soft (individuals' emotions, perception, capability, etc) factors.

Communication failures often occur because either 'pull' or 'push' overdominates in the communication process. This is most often seen by an overwhelming 'push' approach, where communications continue to be transmitted without reference to (in ignorance, indifference or antagonism) to the audience needs and capabilities. However, overwhelming 'pull' demands can have an equally negative impact on communications where the audience demands for information become a nuisance to, or drain resources from, the communicator.

8.6.4 Decision making

To be an effective communication, the information presented must be of use to its audience in making decisions, which itself is about making judgments about a range of uncertain future outcomes. In many instances, particularly in communications post event, the communication should be providing information to enable decisions that will promote desired actions, activities or behavioral changes. Decision making, in all circumstances, will be greatly influenced by the *perception* of individuals.

It happens too often that the desired outcomes are not received from decision makers. In the process of providing information to a decision maker, through to a decision being actioned there are a number of barriers that require understanding and management (Figure 16).

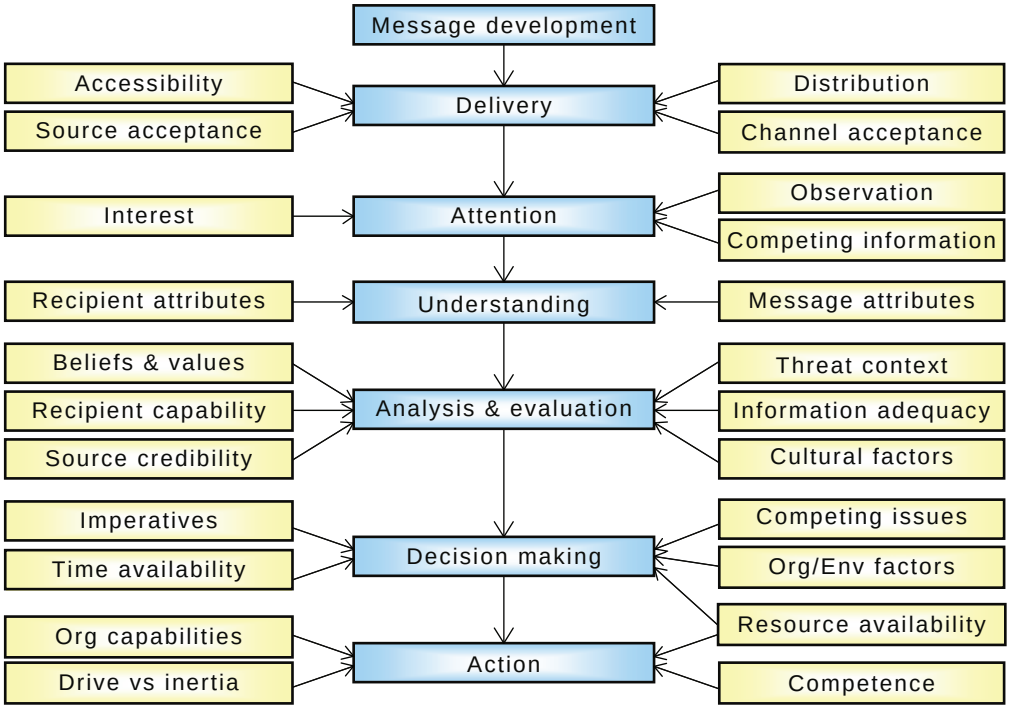


FIGURE 16 ISSUES AND BARRIERS IN COMMUNICATION

Some of the issues that need to be carefully managed include:

- **Message development**

The message needs to be developed with the appropriate level of detail of information, in appropriate language and within the appropriate time frame.

- **Delivery**

To ensure that the message is successfully delivered the information has to be *accessible* and *distributed* to the decision maker (for example delivered at the right time to the right place). Key to this is the decision maker's acknowledgement of the source and of the information and the channel through which it is distributed:

channel acceptance: some decision makers may require their communications to be delivered as a one page brief. A thirty page report or an email may not even reach the stage where it is read by the decision maker.

source acceptance: some decision makers may not accept receipt of the message if they cannot or do not wish to accept the source of the information. For example, messages that have shortcut the chain of command, messages from unknown or un-trustworthy individuals; or information that cannot be verified.

- **Attention**

Information needs to capture the attention of the decision maker. It needs to be initially observed and raise their interest in the midst of significant amounts of competing information. Information that fails to gain attention will forever be pushed to the bottom of the pile.

- **Understanding**

A range of attributes of both the information and of the recipient are critical to gaining understanding. Many of the issues encompassed within CABSMACA (see Table 15) provide a guide to aligning the message attributes with the known attributes of the decision maker. For example, how likely is it that a senior HR manager would have much understanding of a detailed technical report full of electrical engineering terms?

- **Analysis and acceptance**

Capability to analyse the message needs to exist and the output of that analysis needs to be accepted by the decision maker. This includes:

  - recipient capability—the decision maker must have sufficient experience, knowledge and skills to perform analysis on the information,
  - source credibility—the originator of the information must be 'believable' or respected by the decision maker,
  - beliefs and values—information that directly conflicts with existing beliefs or values will be less acceptable and more likely to be disregarded,
  - context—as contexts change the information may be analysed differently or its acceptability may change. Before 9/11 few managers would have regarded information on such suicidal acts as credible,
  - cultural factors—arising from social backgrounds, ethnic origins, educational backgrounds etc will influence how information is analysed and how the results of that analysis will be accepted,
  - information adequacy—the information must be adequate for the type and degree of analysis required of it,

- **Decision making**

Having analysed the information and accepted the output of the analysis, a decision then needs to be made. Issues that will influence the decision itself will include:

  - Imperative—which may constitute organisational priorities (the decision is supported by clear corporate objectives), directional requirements (a whole of government requirement will drive our decision), etc,

- competing issues—for example where emerging issues become more important for a short period of time,
- time availability—time available for making the decision (eg providing detailed information on a complex issue four hours before a decision is required may not be advisable),
- resource availability—perceived future constraints on the resourcing of the outputs that will influence the final decision, and
- other organisational or environmental issues—influences on the decision making process (eg practicalities of installing a new generator within a building's basement area).

- **Action**

Once a decision has been made there are a number of issues that may constrain or prevent it from being actioned or implemented, including:

- resource availability—what appeared to be financially feasible or capable of being resourcing, may not be realistic,
- capability—the organisation may not have the required capabilities or competencies to implement the decision,
- drive versus inertia—although the decision has been made, the organizational or individual will to implement the decision may evaporate.

8.6.5 Perception

Perception is in effect a mental filter through which all information is processed. That information which aligns with our perceptions is usually accepted and further reinforces our perceptions. Information that misaligns with our perceptions is usually disregarded or refuted.

'Regardless of the physical reality of the situation, people will respond to that which they perceive'.*

One type of psychological model suggests that perceptions arise from the way in which the brain processes the information it receives. Information is processed in two ways, through emotional reasoning and through analytical reasoning (Figure 17). The relative balance between these two processes determines the way in which the information is perceived, which in turn will determine to what extent an individual reacts intuitively or with deliberate rational reasoning.

---

* Deborah Pretty, Reputation, Risk and Shareholder Value, April 2003

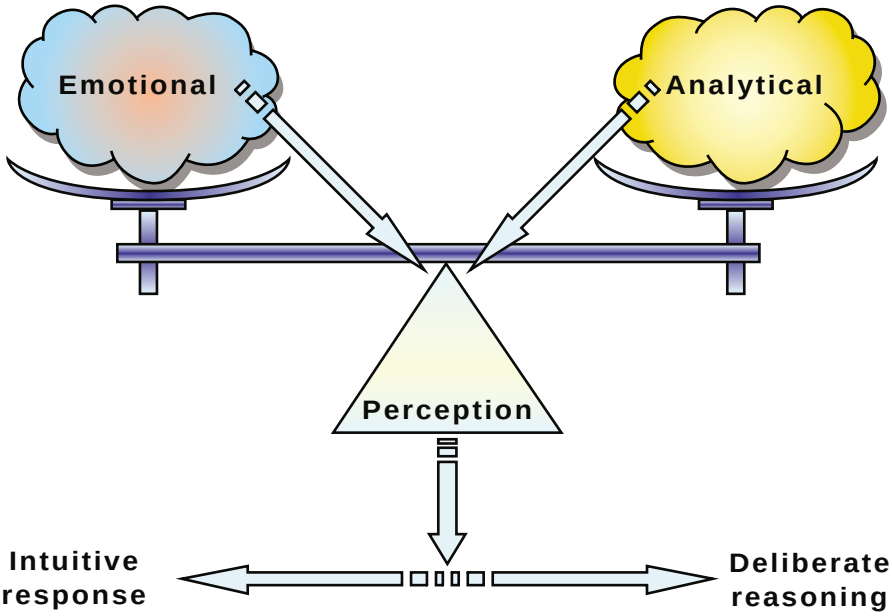


FIGURE 17 THE BASIS OF PERCEPTION

Usually the outputs of analytical and emotional reasoning are 'in balance' – they agree with each other. However, if there is an imbalance – if the emotional outputs disagree with the analytical outputs – the emotional reasoning will usually be the one that wins the day. This goes part way to explaining one of our common failures in communications – where we are trying to change people's behaviour through the provision of facts. Yet we fail to change perception and hence behaviours because the emotional triggers carry more weight than the analytical facts we provide. Perception is influenced by:

- **Personal experience**

Where an issue or event can be related to prior occurrences or experiences, an individual will have a stronger perceptual bias. For example, flood warnings will be perceived at a higher level of danger by those who have previously been victims of flooding, compared to those that have no such previous experience.

- **Perceived extremity**

The relative extremity of an issue or event will significantly alter perception. For example, information regarding an event with exceptionally high or unusual consequences will generally be perceived as more threatening than events with lesser consequences, irrespective of their relative likelihoods.

- **Perceived likelihood**

The most common manifestation of the 'it can't happen to me' paradigm is where the likelihood of an issue or event is believed to be significantly greater or lesser than it really is. Irrespective of the accuracy and strength of the communication and prevailing statistical probabilities, individuals often perceive themselves as immune to the issue or its consequences.

- **Recognition**

Where an individual does not recognise or relate to the issue or event, for example a threat of a tsunami would not have been recognised even as a remote threat by the vast majority of tourists visiting Sri Lanka, Indonesia and other Indian Ocean rim countries in late December 2004.

- **Degree of control**

Where individuals believe that they either can control, or have no control over the issue or event. For example: drivers who are overconfident of their skills while driving at excessive speeds in poor weather and road conditions.

- **Dread and fear**

The level of fear and dread elevates perception of the issue or event beyond all reasonable norms. For example: the perceived risk of flying (arising from a general unease) is greatly amplified following an aviation-related accident or terrorist incident.

- **Proximity of impact**

Where an individual has a physical, cultural, geographical, or social relationship with the issue or event. Perceptions of an overseas disaster change dramatically when even distant friends and family are known to be involved in it.

- **Cueing**

Where perceptions change through heightened awareness and sensitivity arising from increased information from other third parties. This includes:

communicated perceptions of others: for example, peer influence, where panic buying of commodities occurs in a local community when potential shortages are suspected,

media influence: which occurs when the media provide continuing overly-sensational reporting or dramatic images relating to specific issues and events, and

collective consciousness: where perceived risks associated with an issue or event become the accepted and embedded view within a group or society. For example, a view held in some sectors that the major catastrophes are the only ones that can hurt business and so are the only ones that need to be planned for.

- **Beliefs, emotions and value**

Where perceptions are directly influenced by both personal and organisational cultural factors such as beliefs, emotions and values.

8.6.6 The influence of perception

The influence of perception in business continuity management is of paramount importance. It will ultimately determine the decisions that are made at critical points in both planning and response (see Table 18).

Table 18
The influence of perception

Issue	Influence
Perception of context	Issues of critical importance to the organisation are not considered appropriately. The focus of BCM becomes misaligned with 'real' business priorities.
Perception of threats and risk	Inappropriate priorities given to risks, planning may focus on lower level risk, while more realistic higher risks are overlooked.
Perception of business impacts	Impacts of disruption are undervalued or overvalued resulting in inappropriate focus of planning and misallocation of resources.
Perception in strategy development	Strategies are developed for relatively unimportant scenarios while key issues are overlooked.
Perception in testing and exercising	Testing and exercising focus on inappropriate areas resulting in poor validation of plans for effectiveness in the current and likely future environments.
Perception versus reality	The results of analyses are taken as reflecting 100%'reality' and decision making is undertaken on this false premise.
Perception in differences of opinion	Differences of opinion become regarded as expressions of error or as disruptive argument and hence become ignored. For example different perceptions of technical experts and local communities where heightened perceptions may reflect genuine concerns and issues.
Alignment of perceptions	Where differences occur, there is often an attempt to align the 'community perception' with the 'official perception' through approaches such as providing reassurance. Such approaches rarely succeed.
Altering perception through design	The design of processes, structure and communications can often have unexpected (and unwelcome) effects on perception.

8.7 Summary

- **Effective communications are essential for:**
  - the conduct of BCM program activities,
  - ongoing maintenance of the program, and
  - stakeholder communications following the disruption and during the response.

- Detailed written communication plans should be developed consistent with the CABSMACA principles.
- Care needs to be taken to ensure that information gaps between organisational delivery and stakeholder needs are appropriately managed.
- In developing communications plans, the basis of effective communication needs to be understood and these issues addressed:
  - engagement,
  - participation,
  - information transfer, and
  - perceptions.

To assist in the implementation of the *Developing the Communications Strategy* step, a checklist is provided at Section 8.8.

8.8 The communications strategy checklist

		Activity status				
Element	**Issue**	**Not started**	**Delayed**	**On target**	**Completed**	**Comments**
Requirements	Communication requirements have been identified both pre-event and post-event					
	Stakeholders have been consulted in the development of communications plans					
	Required communications have been scoped and prioritised					
	The principles of effective communication have been considered and implemented					
Communications plan	A written communications plan has been developed					
	The plan considers the application of the CABSMACA principles					

9 Maintenance of BCM

9.1 Introduction

A great deal of time, energy and budget can be applied to the development of plans in BCM. However, when a potentially disruptive event occurs and plans are activated they often fail to live up to their potential or expectations. Commonly, after all of the development effort is applied, the plans are placed in drawers or on shelves and left until the 'fateful' day arrives. Plans can date very rapidly (particularly contact lists). Even after a few weeks, if not updated, the effectiveness and relevance of plans begin to deteriorate. Furthermore, although plans may accurately reflect the status quo, they will remain as pieces of paper unless the relevant people within the organisation understand them and know how to use them.

An active and regular maintenance program is therefore required if plans are to remain 'fit for purpose' until required.

An effective maintenance program is built on three key principles:

- People need to understand the need for business continuity, what the plans are for and how to use them. This requires that the capability of the people is maintained, for example through training and exercising;
- Resources (people, information and property*) and process are available and accessible to perform critical business functions. This requires that the capability of the organisation is maintained, through planning, resource management, exercising and business improvement;
- Assuring that the level of understanding and performance is appropriate to the organisation's needs. This requires that the capabilities of these activities are verified and validated through regular monitoring, review, audit, testing and exercising.

---

* Property includes all physical infrastructure and assets.

These three principles provide a *maintenance triangle* for the BCM programs and BCPs (Figure 18). Remove any one side of the triangle and the maintenance will be ineffective.

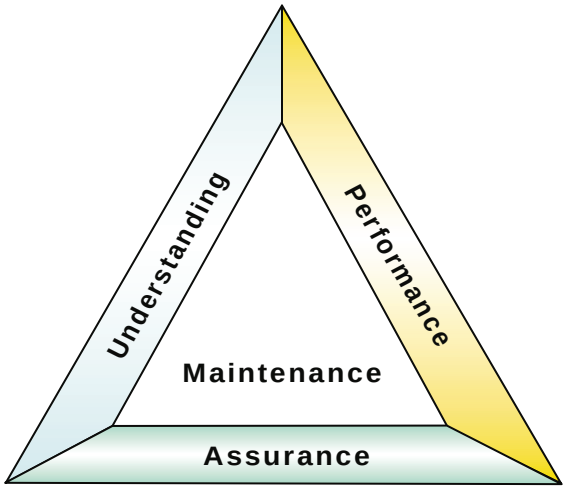


FIGURE 18 THE MAINTENANCE TRIANGLE

9.2 Understanding: training and awareness

Developing understanding and capability can be achieved through a variety of approaches. No one approach will provide an organisation with the people capability it requires. A mix of approaches, appropriate to the context of the organisation is required. These approaches include:

- Awareness;
- Theoretical training; and
- Practical training – exercising.

9.2.1 Awareness

Awareness approaches are usually aimed at providing a broad cross-section of staff with a general understanding of the subject matter. This may be focused on awareness of the BCM program, for example to inform staff of what is happening, what the objectives of BCM are, what the expected outcomes are and what the organisation requires of its people. The awareness approach may be further extended to provide high-level information on the scope and content of individual plans. A more detailed consideration of awareness issues is provided in Chapter 2.

9.2.2 Theoretical training

Theoretical training is normally aimed at providing a higher level of understanding to individuals more intimately involved in BCM. For example, training may be provided to develop or enhance the technical capabilities of staff from within the business who have responsibility for, or will be involved in for example:

- Conducting risk and business impact assessments;
- Developing strategies;
- Writing plans and or implementing plans;
- Conducting media liaison; and
- Operating an emergency operations centre, etc.

Theoretical training therefore needs to be targeted to meet the specific aspects of each of these different needs. A typical approach to theoretical training is summarised in Table 19.

Table 19
Example program for BCM theoretical training

Audience	Subject	Content
Business continuity managers	What is Business Continuity Management?	• Background to BCM. • Nature of crisis and disasters. • Evolution of concepts. • Relationships to other approaches & disciplines. • Core competencies. • Introduction to generally accepted practices.
	How to develop a BCM program	• Identifying the need. • Gaining commitment. • Gaining engagement. • Developing the business case. • Program structure and resourcing issues.
	Risk Management	• Risk and uncertainty. • Generally accepted risk management practices. • Risk controls and treatments. • Relationships between risk management & BCM. • Conducting the risk and vulnerability assessment; and • Using information from the risk assessment.
	Business Impact Assessment	• Principles of the BIA. • Addressing communications issues. • Conducting the BIA. • Capturing information. • Understanding the implications of MAO, RTO and RPO; and • Identifying alternate solutions.
	Developing and documenting strategies and plans	• Developing strategy options for: – emergency response, – continuity phase, – recovery phase; • Consolidating and mapping resources; and • Documenting plans.
	Communications	• Principles of effective communications. • Managing stakeholders. • Developing a communications plan.
	Maintenance	• Maintaining the BCM programs: – conducting awareness and training; – strategies for exercising plans; – establishing an assurance and audit regime; and – reviewing, updating and improving the program and plans.

(*continued*)

Table 19 *(continued)*

Audience	Subject	Content
Plan coordinators	Introduction to BCM	• Background to the history and principles of BCM. • Key organisational priorities. • Structure of the BCM program.
	Risk	• What is risk? • Conducting a risk assessment.
	Business Impact Analysis	• Purpose of the BIA. • Gathering information for the BIA.
	Strategy options	• Understanding options available to manage disruptions.
	Writing the plan	• Information requirements. • Sources of information. • Plan structure and format. • Documenting the plan. • Desk checking.
	Plan audit	• Audit issues and assurance.
Communications specialists	Introduction to BCM	• What BCM aims to provide. • Organisation's approach to BCM. • Relationship to other functions such as emergency management, security, etc.
	Plan coverage	• Scope and responsibilities for plans. • Project disruption responses and activities.
	Disruption communications	• Principles of effective communications. • Communications during disruptions, crises and disasters. • Developing communications plans.
	Plan audit	• Expectations for future audit and assurance activities.
Senior management	Introduction to BCM	• External and internal drivers for improved management of disruptions. • Basic principles of BCM. • Overview of organisational approach to BCM. • Cost implications and benefits.
	BCM program	• Key features of BCM structure and operations within the organisation. • Specific senior management roles and responsibilities. • Overview of other roles and responsibilities within the structure. • Command, control and coordination arrangements.
Other management, staff and key stakeholders	Introduction to BCM	• Overview of drivers for improved management of disruptions. • Basic principles of BCM. • Overview of organisational approach to BCM.
	BCM program	• Key features of BCM structure and operations within the organisation. • Specific senior management roles and responsibilities. • Overview of other roles and responsibilities within the structure.
	Understanding the plans	• Intent and structure or individual plans. • Using plans following a disruption.

9.2.3 Practical training—exercising

Practical training is aimed at improving abilities and confidence in the activation and implementation of strategies and plans. Exercising provides one of the most effective types of this training. The objectives and desired outcomes for undertaking training, through exercising, include:

- Providing staff and key third parties with improved awareness of the content of plans and their use;
- Providing staff and key third parties with enhanced confidence in using the plans and in operating during a disruption;
- Identifying inadequacies in the written plans and in their interpretation by staff;
- Assessment and confirmation of the feasibility of the strategies;
- Assessment of the adequacy of resource allocations and logistics;
- Meeting regulatory, contractual or organisational governance requirements on plan adequacy;
- Providing assurance that plans can be implemented effectively when required; and
- Providing confidence in capability to stakeholders.

9.2.4 Exercising versus testing

The term ‘testing’ is often used in place of, or in conjunction with, exercising. Testing however conveys aspects of ‘pass’ and ‘fail’. It is a natural human desire to avoid failure, with the effect that some individuals will be less than forthcoming about the capabilities of their plans and may try to cover up any ‘weakness’ that they perceive to be present. Such a mindset also dramatically lowers the training and confidence benefits that should arise from participation in a well-conducted exercise. The term exercising is therefore used in an attempt to alter this paradigm and enhance the concepts of rehearsal. Exercising should be conducted in a manner that gradually increases the tension on the plan until ‘weaknesses’ become apparent, but without conveying the impression that it is ‘bad to fail’. Testing of plans can be *one* of the acceptable outcomes of an exercise.

There are a number of different approaches or regimes that can be adopted to exercise plans (relative cost benefits summarised in Figure 19 below):

- **The desktop review:**

The desktop review is also used as an assurance review and will hence often be viewed as a traditional type of test. This would normally be conducted as a physical examination of the documentation to ensure completeness and readability. Desktop reviews are often conducted by a central coordination function. Wherever practical those people expected to use the plan during a disruption should be provided with this opportunity to participate in this review of the plan.

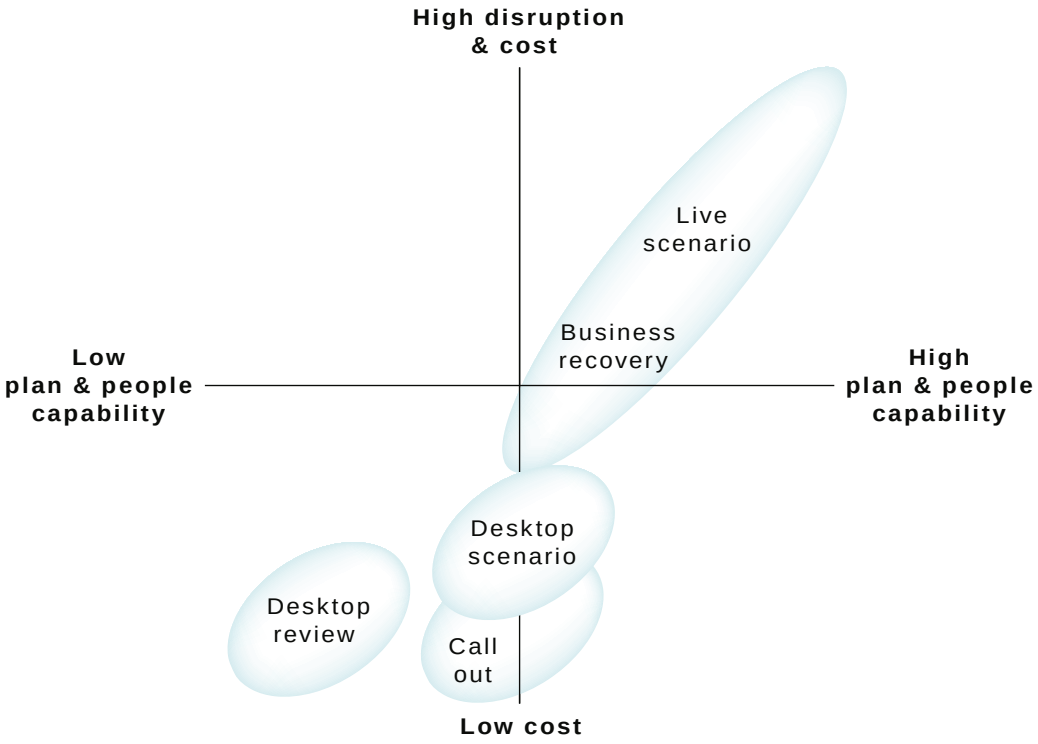


FIGURE 19 RELATIVE COST – BENEFITS OF DIFFERENT EXERCISE REGIMES (EXAMPLE ONLY)

- **Desktop walkthrough**

This provides those individuals allocated responsibilities under the plan with a guided presentation and discussion on the content of the plan and how it would be expected to be used in the event of an activation.

- **Desktop scenario exercise**

Similar to the desktop walkthrough of the plan, it involves an examination of how the plans will be used to guide actions and decisions following activation. The key difference is that rather than a simple discussion of the plan document, this exercise uses hypothetical disruption scenarios to examine assumptions made during the development of the plan.

- **Call out and notification communications exercise**

This involves a physical call up of key contacts and/or deputies identified within the plan and the activation of relevant call out trees. It provides participants with an appreciation for the needs and difficulties in initial communications following an incident. The exercise also provides an opportunity to test the currency and effectiveness of those initial communications plans.

- **Recovery exercise**

This involves either closing down or removing access to key elements of systems or infrastructure. Both the recovery of lost systems/infrastructure and establishment of alternate capability are often examined in this exercise. Note that the exercise need not be limited to exercising IT systems alone, but can be extended across the spectrum of the organisation's infrastructure.

- **Live scenario exercise**

This involves the live activation of plans usually based on a hypothetical scenario. The exercise can be conducted as a limited activation, involving only a few plans; the activation of only parts of individual plans; or can involve full scale activation across the whole organisation.

Exercises of this nature provide an excellent mechanism for examining the interaction and interdependency between individual plans. Although this form of exercise offers the most robust training and examination of the plan, it does make significant demands upon the organisation in both the planning and in the conduct of the exercise. The exercise needs to be conducted with great care as untoward and serious disruption of the business can otherwise occur.

9.2.5 Key exercise considerations

To ensure the effectiveness of the design and conduct of exercises, the following issues need to be considered:

- The exercise is capable of examining issues that will verify plans are practical, feasible and up-to-date;
- Participation in the exercise is capable of promoting increased familiarity of the plans for those individuals with responsibilities under the plans;
- The exercise will provide appropriate assurance that key individuals understand their roles and responsibilities during a disruption;
- The exercise will be able to confirm that resource requirements and key contacts are appropriate to the task at hand and are current;
- The practical issues regarding implementing and managing alternate workarounds will be examined during the exercise;
- Staff will be appropriately and adequately rehearsed in the activation and implementation of plans; and

- Outputs from the exercise will be capable of driving continuing improvement and maintenance of the plans.

The secret to success in exercising plans is to choose and develop realistic scenarios that the participants can relate to. Doom-laden scenarios that result in near total destruction of both the organisation and the surrounding communities will often not be taken seriously by participants. Furthermore, such scenarios will probably not provide an effective realistic pressure for exercising of the plans. Some of the best desktop and live scenario tests are those based on the prior experience of the organisation, or even competitors in the same market or industry. Ideas for scenarios can be found by searching historical records such as accident and incident reports, audit reviews, management reports, etc.

9.2.6 Developing and conducting an exercise

An in-depth consideration of developing and conducting exercises is out of the scope of this Guide. A detailed and concise booklet on managing exercises is available from Emergency Management Australia*. The approach comprises six key steps in the process (Figure 20) and although developed for emergency management exercises, the structure is highly relevant for the conduct of BCM exercises.

These six steps of exercising comprise:

- **Need**

Establishing the organisational need to conduct the exercise, eg to train staff, to familiarise key managers with the content and use of plans, to validate key assumptions within the plans, etc.

- **Analysis**

Involves examining the organisational need in order to define the aim of the exercise. This also involves confirming that this aim will really meet the need and that it is clearly in line with key stakeholder expectations. Implicit within the analysis is a consideration of factors affecting the aim and scope of the proposed exercise, including:

- type of scenario,
- time availability and constraints,
- size and complexity,
- budget and costs,
- equipment,
- regulatory and policy issues,
- people involved,
- areas of the organisation to be involved,
- location of exercise activities,
- other organisations involved,
- logistical support,
- administrative support.

---

* *Australian Emergency Manuals Series. Part V The Management of Training. Manual 2: Managing Exercises, Emergency Management Australia, 2001*.

- **Design**

Design of the exercise involves:

- selecting the type of exercise (eg desktop, simulation, etc),
- creating the scenario,
- developing the storyboard and schedules,
- developing scripts,
- identifying facilitators,
- developing communications & notifications,
- implementing exercise, arrangements and administration,
- creating documentation.

- **Conduct**

Key requirements in the conduct of the exercise include:

- running briefings or participants
- appropriate resourcing
- access to key locations, equipment and so on,
- presence of independent observers (eg Internal Audit),
- clear, concise in exercise communications,
- protocols for termination of the exercise.

- **Debrief**

Debriefs can be conducted immediately at the end of the exercise (so called ‘hot wash’), or sometime later when all parties’ views can be collated and discussed in a suitable forum. Debriefs should address: elements that worked well and those that did not, learnings for the future, improvements to plans, training future exercises, etc.

- **Validation**

Involves assessing the conduct of the exercise and confirming to what extent the aims of the exercise have been achieved.

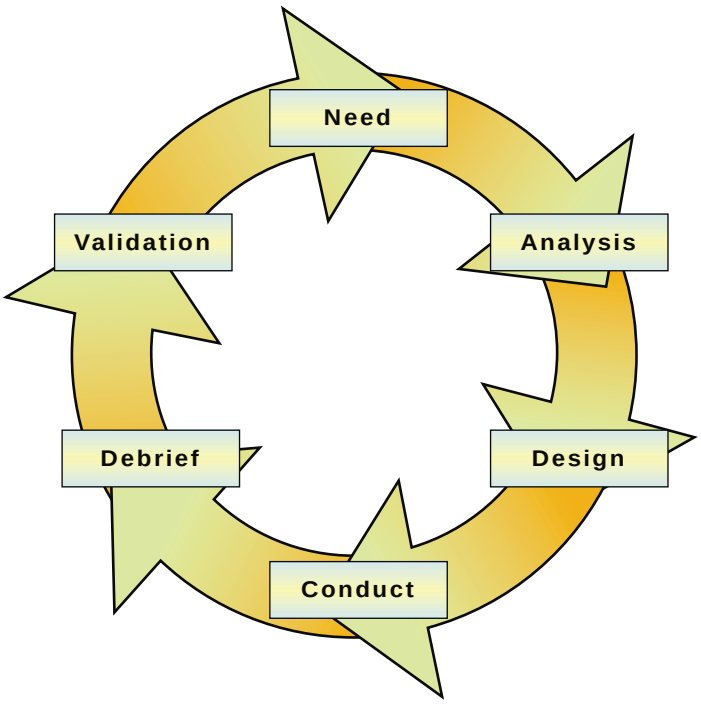


FIGURE 20 THE EXERCISE MANAGEMENT MODEL*

9.3 Performance

The second critical component is ensuring that an acceptable level of performance is maintained as the organisation and its environment change through time. This requires that the existing organisational capability is kept aligned to the evolving needs of the organisation. Fundamental to this is the establishment of an effective process of regular monitoring and review.

9.3.1 Monitoring and review

The main focus of monitoring and review will be upon the documented plans themselves. However, the relevance and effectiveness of BCM as a whole may significantly change over time, and should therefore be included as part of the intended maintenance program.

---

* Based upon *Australian Emergency Manuals Series. Part V The Management of Training. Manual 2: Managing Exercises, Emergency Management Australia, 2001*.

The maintenance program should be based upon a regular cyclical process of monitoring and review where plans and programs are formally updated at least annually. However, significant changes in the internal and external environments will not occur on a regular periodic cycle. Therefore, a well founded BCM maintenance program should also include monitoring for these unanticipated changes which will need to trigger review and update of the plans. Examples of these 'trigger' changes (Figure 21) include:

- **Environmental change**

Changes in the external or internal environment that alter existing disruption risks or create new ones.

- **Strategic change**

Changes in the strategic direction or priorities such that the relative importance of critical business objectives is materially altered.

- **Resource and capability change**

Availability or access to identified resources and/or people or process capability changes.

- **Stakeholder conditions**

Requirements of stakeholders (eg contractual) or their capability to interact with the organisation (eg loss of a unique supplier capability) changes.

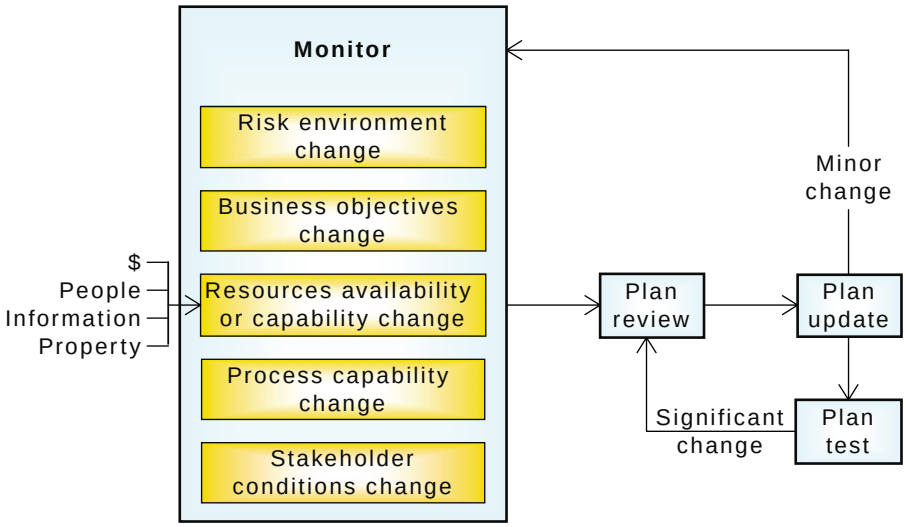


FIGURE 21 TRIGGERS FOR REVIEW AND UPDATING OF BCPS (EXAMPLE ONLY)

Changes to any of these factors may require the plans to be updated. However, where major changes occur, this may require a thorough review of the entire plan. Depending upon the nature of changes observed and the degree of redrafting required, it may be necessary to undertake additional exercising and assurance of the plan in whole or in part.

Key maintenance processes should include the conduct of:

- Confirmation of strategic direction and business objectives;
- Reviews of risks and disruption scenarios;
- Reappraisals of business impact assessments;
- Re-examinations of resource requirements and allocations;
- Confirmation of roles, responsibilities and contact details;
- Reviews of contractual relationships with third parties; and
- Reviews of other interrelationships with third parties.

9.4 Assurance

The third side of the triangle (Figure 18) is assurance which is aimed at providing verification and validation that both the BCM activities and the documented plans are appropriate to the needs of the organisation, i.e. that they are 'fit for purpose'. The combined outcomes arising from assurance activities must initially establish a baseline from which future changes in capability can be measured. This provides both a comparative performance measure (for example to demonstrate that continuous improvement in BCM is occurring) and will demonstrate any relative changes in the organisation's capacity to achieve its desired outputs and outcomes for BCM.

Furthermore, assurance should also demonstrate to both the organisation and to the stakeholders that expectations are being met. Assurance should highlight excellence in performance, identify areas where improvement is required, and inform people about better practices. Assurance activities that are aimed solely at 'catching people out' (the 'gotcha' audit mentality) can seriously undermine the confidence of all parties involved and ultimately lower the effectiveness of the BCM program as a whole.

A range and hierarchy of assurance activities exist (Figure 22) that comprise:

- Component testing

Involving simple checks on specific parts or components of a plan or the BCM program (eg conduct of telephone call outs, self assessments on quality and currency of documented plans, self assessments conducted by the owners of plans, etc).

- Technical assessments

More detailed examinations on plan capabilities (eg IT system recovery tests, activation of emergency operations centres, etc).

- Desktop scenario tests

Involving an assessment of capability and performance during the conduct of desktop exercises of individual plans or groups of interrelated plans.

- Live simulation testing

Involving an assessment of capability and performance conducted during a live simulation exercise.

- Performance audit

Involving a thorough and detailed evidence-based examination of the BCM program and documented plans, usually across a whole organisation or discrete functional areas.

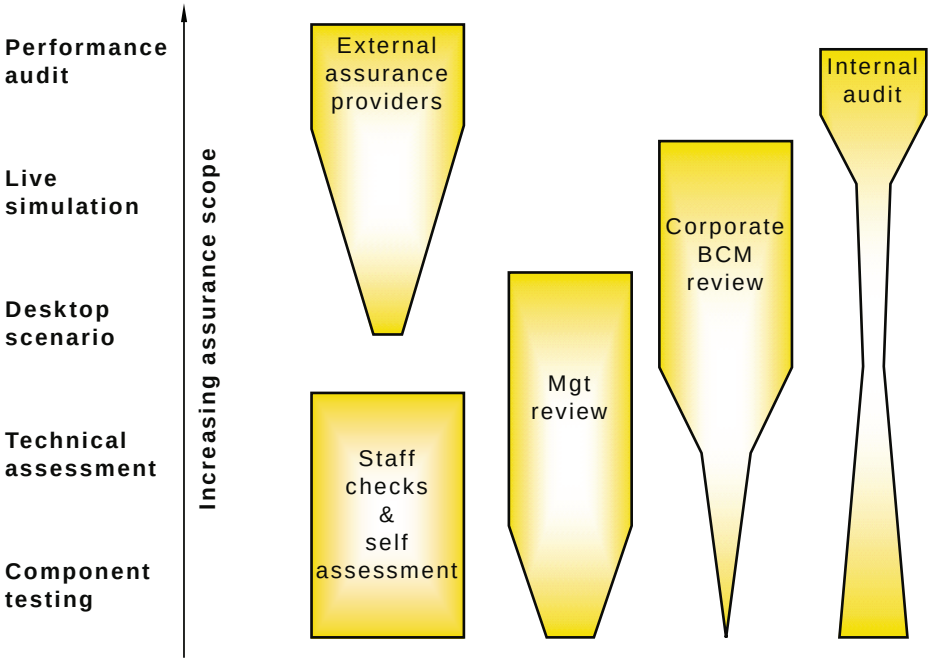


FIGURE 22 THE HIERARCHY OF ASSURANCE APPROACHES (EXAMPLE ONLY)

9.4.1 Assurance scope

The combination of assurance approaches selected should provide a comprehensive examination of each of the key elements of the BCM program and associated plans over the required time frame. Reliance on a single approach, even if it covers the necessary scope will, generally, not provide adequate assurance. Whatever assurance structure is chosen, the following assurance issues will need to be examined (Table 20).

Table 20
Assurance issues and evidence

Assessment item	Issues to consider in the assessment
1 The business continuity management policy and structure	
1.1 Development of the BCM Policy	• 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 Policy coverage	• 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 & deliverables of the business. • The management and conduct of the business continuity program is documented. • Clear responsibilities are assigned to named individuals for the conduct of the business continuity program. • Formal accountabilities are assigned for the business continuity program (including any needs for formal authorisations etc). • The policy describes minimum requirements for a regular monitoring and testing program of the business continuity program and BCPs. • The policy identifies named individuals or job functions for whom reports are required for: – monitoring of plan status and maintenance, – results of testing and exercising of plans, – review, updating and improvement of plans.
2 Business continuity program governance and structure	
2.1 Senior management understand and support	• Documentation evidencing that senior management have been briefed on the program and have given their approval and support. • Involvement of senior management as champions of the business continuity program. • Senior management allocating specific resources (people, time budget, etc) to the achievement of business continuity objectives.
2.2 BCM program plan	• 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.

(*continued*)

Table 20 (*continued*)

Assessment item	Issues to consider in the assessment
2.3 BCM scope	• The policy, BCM strategy project plans, or other documents (identified) specifically identify those areas or critical business functions of the business that require plans 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.
2.4 BCM structure and processes	• The BCM structure and processes are consistent with the principles of accepted industry standards or practices.
2.5 BCM performance	• Formal processes established for the notification and reporting of a disruption. • Documented procedures for conducting testing are in place. • Formal processes for determining the effectiveness of responses to actual incidents are in place.
3 The risk and vulnerability assessment	
3.1 Risk assessment process	• A robust tool is used (eg AS/NZS 4360). • Users of the risk management framework have good familiarity with its use (may involve using expertise from elsewhere in the business or externally for example). • A broad range of potential disruption threats and risks are assessed.
3.2 Risk assessment outputs	• The risk assessment is used to inform the development of potential disruption scenarios. • Assessment of vulnerabilities is conducted either as part of the risk assessment or through a separate vulnerability assessment.
4 The business impact assessment	
4.1 Management, staff and stakeholder involvement.	• Critical business function and process owners/operators have been consulted and/or provided input into the BIA. • Data/information on interdependencies with the other third parties have been included.
4.2 BIA scope	• The BIA has included an assessment and prioritisation of business functions critical to business success. • Business areas providing essential support to the critical business functions have been included.

(*continued*)

Table 20 (*continued*)

Assessment item	Issues to consider in the assessment
4.3 Assessment of disruption scenario impact	The BIA considers: • 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. • Identification and documentation of post-disruption recovery objectives. • Key functional interdependencies.
4.4 Interdependencies	The BIA determines: • Other parties (both internal and external) with which the critical business functions have a relationship. • The nature of those relationships, such as information exchange, delivery/receipt of a service or product, etc. • The level of priority or criticality of those relationships.
4.5 Disruption impacts	• The BIA identifies impacts of selected disruption scenarios/risks on critical business functions. • Evidence that both financial and non-financial impacts are considered.
4.6 Outage times	• Demonstration of a process (eg using information from 4.5 above and determined critical success factors) used to determine outage times. • Evidence of actions or plans aimed at managing significant gaps in outage times, eg gaps between MAOs and RTOs .
4.7 Alternate workarounds and processes	• Demonstration of a process identifying the need for and the development of alternate workarounds and processes. • Evidence that alternate workarounds and processes have been developed in response to identified needs.
4.8 Current preparedness	• Evidence that the findings of the BIA have been reviewed and validated and that the status of current preparedness can be demonstrated.
5 Testing and exercising plans	
5.1 Reaction to an incident	• Demonstration that there is an awareness of and planning to manage the emergency response, continuity phase and recovery phase.

(*continued*)

Table 20 (*continued*)

Assessment item	Issues to consider in the assessment
5.2 Emergency response	• Demonstration that the emergency response strategies are in line with regulations, standards, industry generally accepted practices, organisational policies, etc. • Evidence that strategies address key identified risks.
5.3 Continuity phase	• Evidence of a process for developing strategies that address identified risks and are based upon information derived from the BIA.
5.4 Recovery phase	• Evidence that the longer term recovery needs of the organisation are considered in the planning process. • Demonstration of a process to be deployed for detailed recovery planning post incident.
6.0 Collating and assessing resource requirements	
6.1 Consolidating resource information	• Demonstration of a process for collating and consolidating resource information from multiple critical business functions. • Evidence that resource information is assessed for synergies and conflicts in availability, accessibility, allocation, etc.
6.2 Assessing organisational capabilities	• Evidence that capabilities to manage the disruption are assessed for synergies at a broad organisational level (i.e. across multiple critical business functions and/or plans).
7 Writing the plan	
7.1 Guiding principles	• Plans demonstrate appropriate consideration of the guiding principles in their drafting.
7.2 Framework of plans	• A framework of plans has been developed that is appropriate to the context of the organisation (such as to its size, complexity, geographical dispersion, etc).
7.3 Content of plans	• Demonstration that the content of each plan is comprehensive and meets, where applicable, the requirements of regulations, standards, industry generally accepted practices, organisational policies and procedures, etc.
8 Communications strategies	
8.1 Communications during and after the incident	• Documented objectives and strategies identifying: – who? – what? – where? – when? – why? – how?

(*continued*)

Table 20 (*continued*)

Assessment item	Issues to consider in the assessment
8.2 Written communications plan	• Demonstration of a documented communications plan(s). • Evidence that communications plans follow principles of good communications practice.
8.3 Stakeholders and their needs	• Evidence that the communications needs of stakeholders. have been identified and considered in the development of communication strategies and plans.
8.4 Planning tools	• Evidence that a structured approach has been undertaken to ensure that appropriate: – stakeholders have been communicated and consulted with, – staff (or contractors, suppliers, etc) have been used in developing communications, – levels of authority have been applied to the authorisation of communications.
8.5 Effective communications	• Demonstration of awareness of the basis of effective communications in those people tasked with developing strategies and actions. • Evidence of the application of effective communications.
9 Maintenance	
9.1 Awareness and training of BCM	Evidence of this could include: • Existence of documented training packages. • Conduct of training courses for individuals with BCM responsibilities. • Managers and staff with ownership of critical business functions are exposed to the content of the BCPs. • Participation and attendance in scenario desktop and live simulation exercises.
9.2 Exercise and testing cycle.	Evidence may include: • 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, eg the conduct of a regular 12 monthly review and update cycle.
9.3 Unscheduled plan revision	• Processes are in place to allow for unscheduled revision of BCPs, eg following major structural reorganisations, departure of key staff, etc. • A post-incident review process (eg debriefing) has been established.

(*continued*)

Table 20 (*continued*)

Assessment item	Issues to consider in the assessment
9.4 Performance	• Normal regular monitoring and review processes are in place. • Demonstration that the monitoring and review processes are linked into a regular cycle of update and improvement of plans.
9.5 Assurance	• Demonstration of a structured approach to assurance. • Evidence that assurance activities consider: – the conduct of the BCM program, – the process of plan development, – the content of plans, – the acceptability of plans (eg through exercising), – availability and suitability of identified resources, – understanding and capability of people.
10.0 Activation and deployment	
10.1 Coordination and control	• Evidence that the coordination and control issues have been considered. • Demonstration of coordination and control structure appropriate to the organisations context.
10.2 Disaster kits	• Where disaster kits have been developed, evidence that the composition meets organisation needs.
10.3 Record keeping	• Evidence that appropriate resources, processes and responsibilities have been assigned to record keeping.

9.5 Summary

- **Maintenance of BCM revolves around the concepts of:**
  - Understanding,
  - Performance, and
  - Assurance.
- Understanding (of both internal and external stakeholders) can be achieved through a combination of theoretical training and practical exercising.
- The most effective exercises are those based on the experiences of the organisation, its competitors and its industry.
- Assurance activities need to be undertaken using both ‘internal’ review processes (eg management reviews) and ‘external’ process (eg audit).
- The program and associated plans need to be reviewed on a regular cycle.
- Monitoring processes should be in place to trigger the review of the BCM program and plans when significant changes in the context arise.

To assist in the implementation of the *Maintenance of BCM* step, a checklist is provided at Section 9.6 and a template at Section 9.7.

9.6 The maintenance checklist

		Activity status				
Element	**Issue**	**Not started**	**Delayed**	**On target**	**Completed**	**Comments**
Awareness	Staff have received a broad awareness and familiarisation on the BCM program.					
	Staff have received a broad awareness and familiarisation on the structure and content of plans.					
Training	Nominated staff have received relevant specialist/ technical training (eg in the conduct of the BIA).					
	Nominated staff have taken part in training through the exercising of plans.					
Exercising and testing	A program of exercising and testing has been developed and implemented.					
Performance	The BCM program is subjected to regular monitoring and review of its effectiveness.					
	Plans are subject to regular monitoring and review of their effectiveness.					
	Criteria have been identified and are monitored for triggering the review of plans.					
Assurance	A program or framework of assurance activities is in place to ensure conformance to organisational needs.					

9.7 Exercise template

Template 9.1
Exercise

Business unit:	South East Region
Location:	Big City
Contact name and title:	Dee Mahnd
Telephone:	123 4567
Email:	d.mahnd@ser.org

Each exercise should be given a unique identifying title

Exercise title	Black Storm Five
Plans to be tested	All BCPs for Head Office location
Critical business function/ organisational units involved	All Finance critical business functions All IT critical business functions All Corporate Affairs critical business functions

Identify those parts of the organisation that will be involved

Exercise Location(s)	Curzon House and Data Centre	**Date (1)**	01/09	**Start time**	0800	**End time**	1300
		Date (2)	05/10	**Start time**	1630	**End time**	1900
		Date (3)		**Start time**		**End time**	
		Date (4)		**Start time**		**End time**	

The exercise may be held over several days and at different times

Exercise objectives	
(1)	Rehearse decision making on plan activation
(2)	Rehearse contacts and call outs
(3)	Rehearse removal of personnel to recovery site

Identify what the exercise is aiming to achieve

Resources involved/required
All staff identified in BCPs under exercise Recovery centre Contact lists Emergency communications systems

Identify resources that will be 'exercised'

Exercise exclusions
IT systems and connectivit External stakeholder communications v External stakeholder communications

Identify components of plans and infrastructure that will not be exercised

Support requirements
Admin staff to make recovery centre ready and organise transport Crisis management staff to assist in facilitation Training room for exercise debrief

Identify all support and other resource requirements to conduct the exercise

Exercise facilitator	Ted Roosevelt of Presidential Consulting	**Exercise approved by**	Ima Tabose Deputy CEO

10 Activation and deployment

10.1 Control and coordination of activated plans

Following a major disruption event, there will possibly be one or more emergency response plans activated, multiple business continuity plans, and, progressively over time, a series of recovery and restoration plans (Figure 23). These plans may be competing for resources, time and attention with each other and therefore require a mechanism of overall control and coordination. For this reason, many organisations nominate a number of senior managers to form a control and coordination team (called variously: emergency management team, critical incident management team, crisis team, etc).

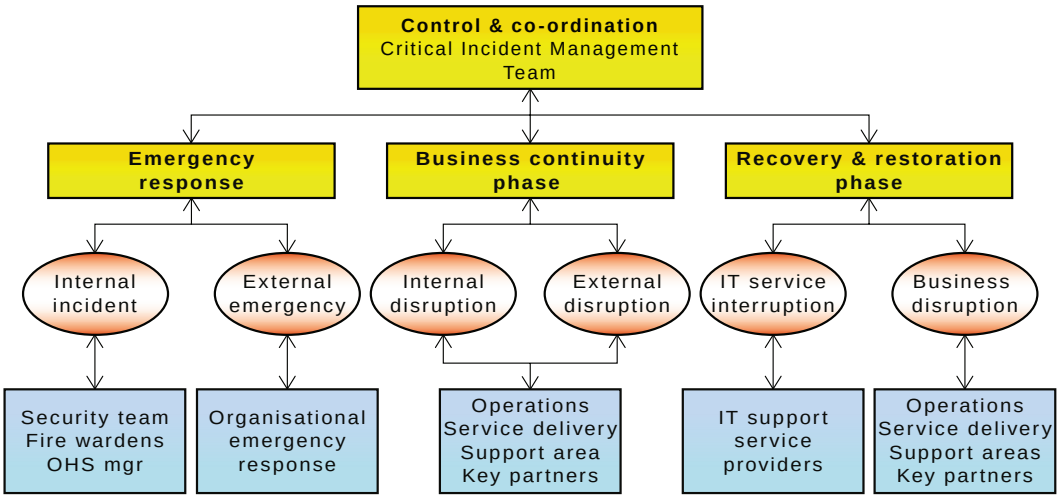


FIGURE 23 CONTROL AND COORDINATION

10.2 Coordination and control framework

Any major disruption event involving multiple contemporaneous or consecutive activities or involving multiple critical business functions can benefit from the application of a formal integrated coordination and control framework.

A generally accepted practice is based upon the 'Incident Control System' (ICS), which has been adopted within Australia as the Australian Interagency Management System (AIIMS*). The ICS is a structured modular role-based framework (Figure 24) that provides a system of predetermined coordination and control activities for the Critical Incident Management Team, with agreed and trained responsibilities and delegations.

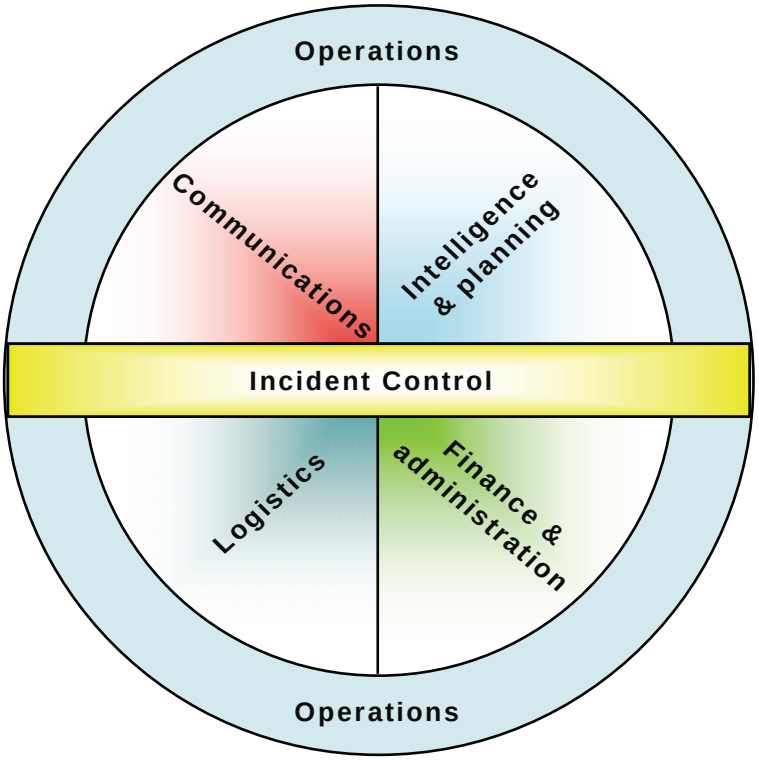


FIGURE 24 AN EXAMPLE OF AN ICS FRAMEWORK

The typical ICS framework is based upon the team leader (Incident Controller) managing with an effective span of control over five other senior managers tasked with specific responsibilities:

---

* *Incident Control System: The Operating System of AIIMs*, Australian Fire Authorities Council, 2nd edition 1994.

- Incident control

The function is responsible for overall management of the incident, a key responsibility is to prepare the objectives for the foundation of subsequent critical incident action planning.

- Operations

The function is responsible for the operational activities associated with the incident, for example, the emergency response and investigations conducted at a major industrial accident, or the activation of business continuity plans for specific functions.

- Intelligence and planning

The function is responsible for the collation of data and information relating to the status of the incident, resource requirements, availability and tasking. The function undertakes analysis of the incident and its current management, maps the progress of the incident and assists in the preparation of strategies to manage the incident.

- Logistics

The function has the responsibility for the provision and management of facilities, accommodation, stores, catering, telecommunications and general support services to operations.

- Finance and administration

The function has responsibility for tracking the cost of the disruption (including any overtime costs), approval of any extraordinary budget requests, purchase of additional equipment and supplies, coordinating the alteration (eg temporary cessation) of non-essential supply items.

- Communications

The function has to deliver three broad requirements:

  - ensuring effective communications through any chain of command that is established to manage the incident and the organisation's response to it,
  - ensuring that staff, contractors and suppliers are kept informed of key issues relating to the incident and its management, and
  - providing information to key stakeholders and the community, and managing the organisation's interaction and involvement with the media.

As the structure is modular it allows the capability to expand to match the requirements of an evolving incident or disruption.

10.3 Building disaster kits

There is never any guarantee that essential information and equipment will be available when required by the critical incident management team. One way of providing some improved capability is to establish 'disaster kits' at the location of the emergency operations (or equivalent), the recovery site and other alternate locations.

A simple disaster kit can comprise:

- Disaster kit storage box;
- Emergency response plans;
- Recovery and restoration plans;
- Staff contact lists;
- CIMT checklists;
- Key document storage files;
- Stationery (notebooks, pens, highlighters, whiteboard markers);
- Filenote logs;
- Critical Incident Management Plan;
- Business Continuity Plans;
- Floor plans;
- Key stakeholder contact lists;
- Document logs;
- Torches, spare batteries; and
- Cab vouchers.

10.4 Record keeping

One of the key responsibilities for the critical incident management is to ensure that adequate records are kept of all key decisions and communications. This may need to be produced for insurers, auditors, regulators, courts, inquiries or the organisation's own post incident debrief. One member of the team should therefore be tasked with collecting such documentation from each team member at the end of each day. Collected documents must be indexed and stored securely. These documents should also prove useful for directing further improvements to strategies, documented plans and in the development of new exercise scenarios and simulations.

10.5 Summary

- An incident could result in the activation of one, several, or many plans affecting one or multiple locations.
- An system for coordinating and controlling the activation, deployment stand-down, and interrelationships between plans to be in place.
- ICS provides an accepted approach for achieving this control and coordination.
- ICS is based upon the concepts of:
  - limited effective span of control,
  - modular structure, and
  - scalability.

To assist in the implementation of the *Activation and Deployment Step,* a checklist is provided at Section 10.6.

10.6 Activation and deployment checklist

		Activity status				
Element	**Issue**	**Not started**	**Delayed**	**On target**	**Completed**	**Comments**
Framework	A framework for the control and coordination of a significant disruption has been established.					
	The framework addresses key capability requirements.					
Roles and responsibilities	Specific responsibilities have been assigned within the framework.					
	Tasked managers are aware of their responsibilities.					
	Tasked managers have been trained in the activation of plans and in the management of a disruption incident.					
Disaster kits	Disaster kits have been established and located at each relevant location.					
	The content of the disaster kit meets key organisational requirements.					
Governance	Requirements for log keeping and control of documentation have been identified and assigned.					
Debriefing	Requirements for post-incident debriefing of managers and staff have been developed.					

A Communication channels

Channel	Advantages	Disadvantages
Staff briefing (face to face)	• Allows for personal contact. • Allows for two-way dialogue. • Allows leadership to be demonstrated. • Provides opportunities for questions to be answered. • Provides timely information.	• Requires parties to be co-located. • Time intensive. • More difficult to control information flows.
Staff briefing (video/ internet broadcast)	• Provides perception of a personal approach. • Allows for wide dispersal over an organisation. • Delivery is more readily tailored to meet local time constraints. • Can be independent of geographical location of participants. • Relatively low cost for delivery of information.	• Can require considerable time to create the communication. • Significant time demands on spokesperson. • Heavy dependence on technology and access to technical expertise. • Can be high cost to develop message. • Allows for one way flow of information only. • Information is increasingly dated.
Staff briefing (teleconference)	• Relatively easy to set up. • Independent of geographical location. • Allows for two way dialogue. • Provides timely information.	• Less personal interface. • More difficult to provide visual media to accompany primary message.
Press release	• Relatively easy to provide to outlet. • Potential wide distribution to broad range of stakeholders (particularly secondary audiences). • Helps to manage content of media reporting. • Information can become rapidly dated.	• Requires careful drafting. • Little control as to how the press release will be used. • Limited amount of information that can be provided. • High uncertainty regarding effective exposure to desired audience. • Information broadcast is limited to the media's schedule.

Channel	Advantages	Disadvantages
Email	• One message can be sent to tens of thousands instantly. • Almost instantaneous messaging. • Lack of control to resend to secondary and opportunistic audiences.	• Requires people to regularly log on to accounts to receive messages. • Requires access to and general availability of technology. • Limited use for two-way dialogue.
Telephone	• Provides rapid messaging to selected people. • Allows for two way dialogue. • Can be held independent of geographical location. • Can provide timely information.	• Limits on size of audience. • Can be time consuming (controlled by use of call out trees). • Requires operational telephone system. • Requires up-to-date contact lists.
Paid advertising	• Allows for full control of message content. • Allows for wide audience reach.	• Significant lags in delivery of message (depends upon media's production schedule). • Little control over audience uptake. • Little control over audience access. • Limited amount of information can be provided. • Can be a significant cost. • Independent of organisation's technology capability • Provides for one-way communication only.
Posters and notices	• Can be produced even with significant loss of technology. • Can be directed to specific geographical locations.	• One-way communication only. • Time consuming to distribute in any quantity. • Limited geographic distribution. • Can be restricted access to the audience. • Can be difficult to provide up-to-date information.
SMS	• Can provide simultaneous communications to entire contact list. • Provides for rapid communications.	• Very limited two-way communication capability. • Very limited message content. • Requires up-to-date mobile phone contact numbers. • Requires access to an operational mobile phone network. • Requires contactees to have mobile phones in their possession.
Broadcast/ print media Interview	• Allows for rapid communication to large and geographically dispersed audience. • Can provide an organisation with the opportunity to 'tell their side of the story'.	• Communications limited to broadcaster's/ publisher's schedule. • Difficult to control content. • Very limited message content. • No control over audience selection.

Channel	Advantages	Disadvantages
Interactive voice response	• Once established requires limited resources to maintain. • Allows for full control over the message to be delivered. • Provides rapid messaging to inquiries.	• Does not allow for real two-way dialogue. • Messages limited to those that call into the service. • Limited capability for message content.
Hotlines	• Allows for two-way dialogue • Can provide the audience with the 'personal touch' • Can provide 24x7 access • Can provide information 'on demand'	• Resource intensive • In major diasters can have adverse health impacts on call centre staff • Information limited to capabilities of call centre staff • Information can only reach a limited audience • Can disenfranchise parts of the audience if there are contact difficulties or delays.
Newsletters	• Provides for full control over content. • No significant limits on amount and detail of information to be provided. • Timing of release of information under full control of the organisation. • Control over initial distribution of information).	• Once released, limited control over access by opportunistic audiences. • Can be significant time delays and difficulties in distribution. • Requires effort on the part of audiences to read and assimilate information.
Internet and Intranet Sites	• Allows communication with a large geographically dispersed audience. • Allows for rapid dispersal of information. • Can provide paid updates on changing situations. • Content under control of the organisation. • Provide audience with 24x7 access to information.	• Requires access to technology and specialist capability. • Requires audience technological capability to access information. • Can be little control (particularly for internet delivery) over target audiences. • Can be subject to malicious attack: denial of access, corrupted information etc.

B Sources of risk

Table B1
External sources of risk

External sources of risk	Risk issues
Economic	Market growth, economic cycle, shares & interest rates, capital movement, regional stability.
Political and regulatory	Legislation, investment, standards & protocols, acceptable practices, intellectual property.
Supply	Components, outsourcing, contractors, quality assurance, logistics.
Technology	Hardware, software, security, user interface.
Competition	Resources, skills.
Community	Reputation, content, ethics, partners, practices.
Physical	Natural events, location, human error, emissions & pollutants.

Table B2
Internal sources of risk

External sources of risk	Risk issues
People	Knowledge retention, skills, integrity, loyalty, industrial relations.
Data/information	Integrity, currency, relevance, access, storage.
Strategy	Robustness, flexibility, strategic fit, planning, capability, implementation.
Stakeholder management	Stakeholder needs, segmentation, fulfilment, relationships, service proposition.
Leadership	Vision, management capability, innovation, culture.
Process/product/services	Robustness, capability, intellectual property, life cycle, innovation.
Business results	Business objectives, growth, sustainable development.

C Example of a priority triage rating framework

Level	Score	Minimum acceptable outage time	Contribution to critical business objectives	Risk of loss of availability	Critical success factor criteria
Gold	5	<24 hours	**Essential**: business objective will not be achieved if CBF is unavailable.	**Extreme:** loss of CBF represents extreme risk to organisation.	**<24 hours**: Critical success factor dependencies of 48 hours or less.
	4	<48 hours	**Major**: achievement of business objective will suffer lengthy delays or experience major deterioration if CBF is unavailable.	**High:** loss of CBF represents high risk to organisation.	**<48 hours**: Critical success factor dependencies of 48 hours or less.
Silver	3	< 1 week	**Moderate**: achievement of business objective will suffer material delays and/or will experience moderate deterioration if CBF is unavailable.	**Significant:** loss of CBF represents significant risk to organisation.	**<1 week**: Critical success factor dependencies of 1 week or less.
Bronze	2	1-4 weeks	**Minor**: achievement of business objective will suffer delays and/or experience minor deterioration if CBF is unavailable.	**Medium:** loss of CBF represents low risk to organisation.	**<1-4 weeks**: Critical success factor dependencies of between 1 to 4 weeks.
	1	> 1 month	**Minimal:** achievement of business objective will suffer slight delays and/or will experience minimal deterioration if CBF is unavailable.	**Low:** loss of CBF represents low risk to organisation.	**> 1 month**: Critical success factor dependencies of 1 month or more.
Non critical	0	No requirement for MAO	**Insignificant:** Delays to achievement of business objective are regarded as unimportant and/or experience insignificant deterioration if CBF is unavailable.	**Negligible**: little or no discernable risk is recognised.	Critical success for the CBF has no time dependencies.

D Example threats and hazards

Threat/ hazard category	Potential threat or hazard	
Commercial and legal relationships	• Litigation. • Strike. • Product contamination/ liability.	• Contractual clauses. • Supply chain. • Insurance claim.
Economic circumstances	• Financial. • Interest rates. • International trade.	• Foreign currency rates. • Hedging. • Spot prices.
Human behaviour	• Terrorism. • Fraud. • Theft. • Trespass. • Misappropriation. • Bomb/bomb threat. • Civil disturbance or riot. • Extortion. • Armed hold up. • Kidnap/ abduction.	• Siege. • Human error. • Sabotage. • Mass casualty incident. • VIP situation. • Crowd surge. • Civil disturbance. • Industrial action.
Natural events	• Flood. • Drought. • Earthquake. • Bushfire. • Hurricane/ cyclone. • Tornado. • Storm. • Thunderstorm.	• Snow fall/storm. • Severe rainfall. • Ice storm. • Severe cold. • Severe heat/humidity. • Smog. • Pandemic.

Threat/ hazard category	Potential threat or hazard	
Political circumstances	• Government policy/ direction. • Government instability.	• Changes in legislation/ regulation. • Regulator involvement in industry sector.
Technology and technical issues	• Computer damage (hardware). • Computer damage (software). • VESDA failure. • Application failure/ loss. • Air conditioning loss. • Transport. • Utilities failure. • Information loss. • Virus. • Electrical failure. • Generator failure. • Transportation failure. • Fuel shortage. • Natural gas failure.	• Medical vacuum failure. • HVAC (Heating, Ventilating and Air Conditioning) failure. • Information systems failure. • Fire, internal. • Flood, internal. • Hazmat exposure, internal. • Supply shortage. • Structural damage. • Building loss. • Water failure. • Sewer failure. • Steam failure. • Fire alarm. • Communications failure. • Medical gas failure.
Management activities and controls	• Fraud. • Negligence.	• Misappropriation.
Occupational health and safety	• Staff, public or supplier injury or death. • Contamination of air supply. •	• Contamination of air conditioning system. • Water contamination.
Property and other damage	• Structural damage. • Loss of building/ facility/ asset • Collateral damage. • Fire. • Explosion. • Hazardous material incident. • Radiologic exposure.	• Vandalism. • Flood. • Vermin. • Accidental collision. • Poor maintenance. • Wear and tear. •
Environmental	• Degradation.	• Pollution discharge.

E Vulnerability assessment – Issues for consideration

Category	Control issue	Example vulnerability
Socio-economic–political	Legislative drivers for BCM.	• Absence of legislation mandating/ recommending requirements contributing to improve sustainability &/or continuity of operations.
	Compliance with regulatory requirements.	• Current non-compliance with key regulations (eg OHS).
	Existing continuity measures to meet regulatory requirements.	• No formal processes in place to ensure mandatory reporting of incidents occurs.
	Local political and social stability.	• Increasing political activism, terrorism, civil unrest etc.
	Regional political and social stability.	• Increasing political activism, terrorism, civil unrest, ethnic unrest, protests, environmental issues, etc.
	Exposure to changing regulatory regimes.	• Changes foreshadowed impacting upon areas of operation.
	Economic stability.	• Changes in local economies, market composition, major companies exiting local economy, local companies being purchased by overseas entities, reduction in the number of local manufacturers of required goods and services, etc.
Organisational–strategic	Management commitment to BCM.	• No formal undertaking provided by management. • BCM champion not identified.
	BCM resourcing.	• Resourcing does not meet requirements. • Ongoing BCM resourcing not provided.
	Clarity and understanding of the business and it priorities.	• Management and staff do not demonstrate understanding of key business objectives.
	Extent of organisational buy-in to BCM.	• BCM activity is restricted to only a few areas.

Category	Control issue	Example vulnerability
	Financial/capital structure.	• Insufficient cash flow to cope with immediate needs following a disruption.
	Authorities (e.g. Federal/ State/ Territory/ Local/ Emergency Services).	• Lack of formal delegations, unclear accountabilities and responsibilities.
Local environment	Proximity to high hazard exposures.	• Premises located next to/ in the vicinity of sites (e.g. substation, switching yard, chemical storage, treatment plants, telecommunications, etc).
	Stability of physical/natural environment.	• Location is subjected to frequent severe weather events (flood, bushfire, drought, snowstorm, cyclone, etc).
	Access to information.	• No indication of location of key information resources. • Lack of accessibility to key information resources.
	Public infrastructure resilience.	• Ageing physical infrastructure, frequent loss of utility services (water, power, electricity, gas, telecommunications).
	Robustness of organisational communications systems.	• Communications to stakeholders are ad hoc and unreliable.
	Organisational infrastructure redundancy.	• Critical dependencies on unique plant that is not easily replaced.
	Document management.	• Dependency on unique paper documents. • Unsure of actual number of unique paper documents.
	Dependency on IT systems.	• Key processes are dependent upon availability of IT systems.
	Resilience of IT systems.	• Most processes use legacy systems based on ageing infrastructure (e.g. hardware, software, communications).
	Extent and effectiveness of IT security applications and processes.	• IT security is limited to maintaining server firewalls. • No formal security policies and procedures. • Little or limited changes to IT passwords.
	Extent and effectiveness of physical security arrangements.	• Effectiveness of security measures is untested.
	Extent and effectiveness of people security policies and practices.	• Absence of pre-employment screening practices.
	Alternate/back up sites.	• No alternate sites identified for recovery of business processes. • Alternate sites not reviewed, maintained and tested regularly.

Category	Control issue	Example vulnerability
	Systems of safety.	• Ineffective system of safety, frequent breaches reported.
	Robustness and maintenance of facility physical infrastructure	• Poor housekeeping, facility in poor state of repair.
People	Extent of specialist knowledge.	• Knowledge of a critical process limited to one person.
	Competencies.	• Staff responsible for key business function(s) are new to roles.
	Understanding.	• Staff have not received appropriate BCM training.
	Participation in exercises.	• Exercises have been limited to senior management &/or operational teams only.
	Experience of disruptions.	• Staff have not been previously exposed to live disruptions.
	Industrial relations.	• Ongoing animosity between management and unions/ employee associations and groups.
	Employment relationship.	• Employment agreements restrict redeployment of staff to alternate sites.
	Staff communications.	• Most information is circulated via the rumour mill. • No formalised staff communications system.
	Existing team management arrangements.	• Culture does not promote effective team work.
	Workforce morale.	• Disgruntled workforce, increasing trend in stress claims.
Process and resource defences	Supplier resilience.	• Alternate suppliers available. • Suppliers have adequate BCM in place.
	Contractual conditions.	• Customer requirements for continuity of service cannot currently be met.
	BCM deployment.	• High volume of plans created but no testing/exercising conducted. • Planning does not extend to all locations.
	DRP deployment.	• Recovery tests are not conducted on a regular basis. • DRPs not developed for several applications.
	alternate processes/workarounds.	• Workarounds for key processes are not available.
	Extent of audit and review activities.	• Audit activity does not consider resilience issues. • Audit activity does not determine the effectiveness and appropriateness of plans.

F Document recovery and restoration triage

Document priority	Priority criteria	Example documents
Gold: Priority 1	• Any of the following where no acceptable alternate copies are available: – legislative requirement, – evidential material, – critical business information, – original documents.	• Original legal documents. • Court evidence. • Hard copy payroll adjustment information. • Medical documents including case notes and X-rays etc.
Silver: Priority 2	• Critical business documents where replicas can be obtained from third parties with additional financial outlay and time delays. • Critical business documents where only alternative copies reside potentially in compromised internal storage areas (electronic or physical). • Critical or high value reference documents, out of print publications etc.	• Original letters, case files, multiple source compilations etc.
Bronze: Priority 3	• All documents where acceptable alternate (hard copy or electronic) copies are stored offsite, other low value documents, periodicals etc.	• General business documents, management reports, circulars, text books etc.

G Example of consolidated resource mapping

Table G1
Routine operational requirements

Critical business function	Staff	Desks	PC + SOE	Telecom	Vital records	Transport	Budget $000	Additional facilities	Other requirements
Payroll	3	3	3	3x desk ph. 1x mobile ph.	Payroll file Adjustment forms	Nil	$200	Nil	External data line access
Cheque payments	8	8	8	8x desk ph. 2x mobile ph.	Accounts file Cheque stock	Nil	$1,000	Secure cheque print room	Cheque printer
Threat assessment	1	1	1	1x desk ph. 1x mobile ph.	Security briefs	1 x vehicle	$200	Secure room for analysis Secure document storage	External data line access

Table G2
Disrupted operational requirements

Critical business function	Staff	Desks	PC + SOE	Telecom	Vital records	Transport	Budget $000	Additional facilities	Other requirements
Payroll	1	1	1	1x desk ph. 1x mobile ph.	Payroll file Adjustment forms	1 person to recovery site	$200 + $100 for bureau service	Nil	External data line access
Cheque payments	3	3	3	1x desk ph. 1x mobile ph.	Accounts file Cheque stock	1 person to recovery site	$1,000 + $300 for bureau service	Secure cheque print room	Cheque printer Or referral to bureau
Threat assessment	1	1	1	1x desk ph. 1x mobile ph.	Security briefs	1 x vehicle	$200	Secure room for analysis Secure document storage	External data line access

H Example of content for other plans

Example of content of a BCP for a small to medium sized organisation.

Front page	• Name of organisation. • Name of group/ team. • Name of BCP. • Version number. • Month/Year of plan.
Table of contents	• Review and distribution lists. • Plan authorisation. • Purpose of plan. • Assumptions or limitations of the plan. • Related documents. • Plan activation: – overview of when the plan will be activated & implemented, – escalation triggers, – identify detailed checklists in Appendices. • Location of alternate facilities &/or accommodation. • Resources requirements. • Appendices: – emergency response checklist, – continuity checklist, – recovery checklist, – systems/ specific items details, – contact details, • internal, • external.

Glossary of terms

Activation

When all or a portion of the business continuity, emergency or recovery plan have been put into motion.

Alternate site

An alternate operating location to be used when the primary facilities are inaccessible.

1) Another location, computer centre or work area designated for recovery.
2) Location, other than the main facility, that can be used to conduct business functions.
3) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event the primary site is not available.

SIMILAR TERMS: Alternate Processing Facility, Alternate Office Facility, Alternate Communication Facility, Backup Location, and Recovery Site.

Alternate work area

Office recovery environment complete with necessary office infrastructure (desk, telephone, workstation, and associated hardware, communications, etc.); also referred to as Work Space or Alternative Work Site.

Asset

An item or process that an individual, community or Government values and is vital to supporting the expectations of those people, organisations or Government's outcomes and objectives.

Audit

The process by which procedures and/or documentation are measured against pre-agreed standards.

Backlog

The amount of work that accumulates when a system or process is unavailable. This work needs to be processed once the system or process is available and may take a considerable length of time to reduce. In extreme circumstances, this condition may become so large it may not be cleared or resolved.

Business case

A usually documented proposal outlining an intended course of action and identifying costs and benefits. Generally seeks an approval and/or budget allocation.

Business continuity

Business continuity is 'the uninterrupted availability of all key resources supporting essential business functions'.

Business continuity management

Business continuity management provides for the availability of processes and resources in order to ensure the continued achievement of critical objectives.

Business continuity planning

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 assets.

Business continuity plans

A collection of procedures and information that is developed, compiled and maintained in readiness for use in the event of an emergency or disaster. (Associated terms: Business Recovery Plan, Disaster Recovery Plan, Recovery Plan).

Business continuity program

An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity services through personnel training, plan testing and maintenance. (Associated terms: Disaster Recovery Programme, Business Recovery Programme, Contingency Planning Programme).

Business Impact Assessment (BIA), also known as Business Impact Analysis

A management level analysis, which identifies the impacts of losing company resources. The BIA measures the effect of resource loss and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning. (Associated terms: Business Impact Assessment, Business Impact Analysis Assessment).

Business interruption

Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organization location.

Business process

Key business processes are those processes essential to delivery of outputs and achievement of business objectives.

Capability

The ability, experience, knowledge, skills ,etc of people and organisations, (including the ability and fitness for purpose of processes, assets, infrastructure, etc) to undertake the desired activities and achieve required outcomes.

Community

A group of people with a commonality of association and generally defined by location, shared experience or function.

Consequence

The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Alternative

The impact on the business, its stakeholders and the environment that would result from a real or potential occurrence of the security threat being considered.

Context

A summary of the key internal and external issues that could influence the risks under examination.

Conformance

A compliance approach to monitoring.

Control

Any physical, behavioural, institutional, or cultural mechanism by which a risk is mitigated.

Corporate governance

A system by which an organisation is directed and controlled. Corporate governance activities are represented as four principal components: direction, executive action, supervision and accountability.

Crisis

An untoward event occurring that potentially or actually results in a disruption to the day-to-day operations of part or the whole of the organisation. Management is required to divert a proportion of their attention, time, energy and resources away from normal operations to managing this untoward event. Crises will and do occur on a regular basis and are usually characterised by being managed by existing internal resources.

Critical business functions

Vital business functions without which an organisation cannot long operate. If a critical business function is non-operational, the organisation could suffer serious legal, financial, goodwill, or other serious losses or penalties.

Criticality

The importance or dependence that an organisation has on a function, process, item or infrastructure or specific facility.

Critical incident management

The policies, structures and processes by which the response to abnormal conditions is commanded, coordinated and controlled.

Customer

An individual, organisation or other body that derives a benefit from an asset.

Declaration

A formal statement that a state of disaster exists.

Disaster

If an incident overwhelms management's capabilities to cope, control will begin to be lost and the event becomes regarded as a disaster. Disasters are usually characterised by external agencies taking over management of the event.

Disaster recovery planning

Disaster recovery planning is often used to refer to those activities associated with the continuing availability and restoration of the IT infrastructure.

Emergency

- An event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response.
- Any event which arises internally or from external sources which may adversely affect the safety of persons in a building or the community in general and requires immediate response by the occupants.
- An unplanned situation arising, through accident or error, in which people and/or property are exposed to potential danger from the hazards of dangerous goods. Such emergencies will normally arise from vehicle accident, spillage or leakage of material or from a fire.

Emergency operations centre (EOC)

- A facility, either static or mobile, from which the total operation or aspects of the operation are managed.
- A facility established to control and coordinate the response and support to an incident or emergency.
- Also known as an incident control centre, agency operations centre and forward control centre.

Evaluation criteria

Criteria such as risk consequence and likelihood levels that are used to determine risk tolerance and appetite.

Event

Occurrence of a particular set of circumstances.

Facility

Any physical infrastructure.

Financial impact

An operating expense that continues following an interruption or disaster, which as a result of the event cannot be offset by income and directly affects the financial position of the organisation.

Hazard

A potential source of harm. The term hazard can be qualified in order to define its origin or the nature of the expected harm.

Impact

The outcome following the occurrence of an event.

Incident command system (ICS)

Combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure with responsibility for management of assigned resources to effectively direct and control the response to an incident. Intended to expand, as situation requires larger resources, without requiring new, reorganised command structure.

Incident response

The response of an organisation to a disaster or other significant event that may significantly impact the organisation, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organisation to a more stable status.

Interdependency

The nature of a relationship between two parties.

Likelihood

Used as a general description of probability or frequency of an event occurring.

Maximum acceptable outage (MAO), maximum tolerable outage (MTO), maximum downtime (MD)

The maximum period of time that critical business processes can operate before the loss of critical resources affects their operations.

Mitigation

The means by which risk is controlled or treated.

Organisation

A company, firm, organisation, association, group or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.

Probability

A measure of the chance of occurrence expressed as a number between 0 and 1.

Recovery

- Process of planning for and/or implementing expanded operations to address less time-sensitive business operations immediately following an interruption or disaster.
- The start of the actual process or function that uses the restored technology and location.

Recovery strategy

A pre-defined, pre-tested, management approved course of action to be employed in response to a business disruption, interruption or disaster.

Recovery point objective (RPO)

The point in time to which systems and data must be recovered after an outage. (e.g. end of previous day's processing). RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that may need to be recreated after the systems or functions have been recovered.

Recovery time objective (RTO)

The period of time required to fully re-establish adequate resource requirements.

Risk

The chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and likelihood.

Risk management

The culture, processes, and structures that are directed towards the effective management of potential opportunities and adverse effects.

Stakeholders

- Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision, activity, or event.
- Includes anyone with an interest or influence in the organisation or community.
- Includes anyone with an interest or influence in the organisation or community (or projects, issues associated with or parts thereof), this could include (but not be limited to): the Board, management, employees, citizens, local communities, unions, shareholders, families, media, lobby groups, customers, suppliers, government, regulators, etc.

Test

An activity that is performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria.

Threat

A measure of how likely a source of threat is to succeed in their activity.

Threat source

A list of potential sources that could cause harm to an organisation. For example, a vandal, a disgruntled former employee, a criminal, stakeholders, customers, or a terrorist.

Vulnerability

In a security context, vulnerability is a measure of the likelihood that various types of security/ control measures (physical, personnel, policies, etc) against a threat source will fail. Vulnerability comprises ‘resilience’ and ‘susceptibility’. Resilience is related to existing controls and susceptibility is related to exposure.

Definitions derived from:

- Australian National Audit Office, Keeping the Wheels in Motion, 2000;
- Business Continuity Management Handbook, HB 221: 2004. Standards Australia/ New Zealand;
- Business Continuity Institute, Better Practice Guide;
- Disaster Recovery Institute International;
- Disaster Recovery Journal;
- Emergency Management Australia Glossary;
- National and international industry practitioners;

J Bibliography

Australian National Audit Office, (2000). Business Continuity Management - Keeping the Wheels in Motion.

Australian Prudential Regulation Authority, (2004). Prudential Standard – BCM (Draft).

Australian Fire Authorities Council, (1994). Incident Control System: in Australia refer The Operating System of AIIMs, 2nd edition.

American Society of Industrial Security International, (2005). Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery.

British Standards Institution, (2003). Publicly Available Specification 56 (PAS 56).

Business Continuity Institute, (2001). Business Guide to Continuity Management.

Business Continuity Institute, (2003). Business Continuity Management - Preventing Chaos in a Crisis.

Business Continuity Institute, (2003). Professional Practices For Business Continuity Planners: Coordination With External Agencies.

Business Continuity Institute, (2005). Business Continuity Management – Good Practice Guidelines.

Disaster Recovery Institute International, (2003), A Professionals Guide to the contents of a Business Continuity Plan & Glossary.

The DRJ Editorial Advisory Board's (EAB) Generally Accepted Business Continuity Practices Committee and Disaster Recovery Institute International, (2006). Generally Accepted Practices (Draft).

Emergency Management Australia, (1993). Commonwealth Counter Disaster Concepts and Principles.

Emergency Management Australia, (1998). Pt III Emergency Management Practice Vol 3 Guidelines. Guide 1 – Multi-Agency Incident Management.

Emergency Management Australia, (2001). Australian Emergency Manuals Series Part V – The Management of Training. Manual Two – Managing Exercises.

Institute for Crisis Management, (2004). ICM Report 2004.

Deborah Pretty, (2003). Risk Culture and Ethics. Institute of Internal Auditors/ AIRMIC (UK) April 2003.

National Fire Protection Association (USA), (2004). NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs.

SPRING Singapore, (2005). Technical Reference - Business Continuity Management for Manufacturing, Innovation and Services Sectors TR-19.

Standards Australia, (2004) HB 221:2004 Business Continuity Management.

Standards Australia, (2002). AS 3745-2002 Emergency control organisation and procedures for buildings, structures and workplaces.

Standards Australia, (2003). AS/NZS 7799.2 (BSI 1799.2), Information Technology Security.

Standards Australia, (2006). Security Risk Management Handbook (in press).

Standards Australia, Standards New Zealand, (2004). AS/NZS 4360 (2004) Risk Management.

K Acknowledgements

The authors wish to express their gratitude to the following individuals who provided useful insight into business continuity management practices, critical advice on the content and our expression of it, and gave encouragement when our energies flagged.

John Bircham, Bircham Global, Hamilton, New Zealand.

Neil Britten, Asian Development Bank, Manila, Philippines.

Ian Clarke, Business Continuity Institute, New Zealand.

Jean Cross, University of New South Wales, Sydney.

Luke Dam, Emergency Management Australia Institute, Mt Macedon.

Adrian Gordon, Canadian Center for Emergency Preparedness, Toronto, Canada.

Pearse Healy – Transport Accident Commission and Victorian WorkCover Authority, Melbourne.

James Kilgour, Canadian Center for Emergency Preparedness, Toronto, Canada.

Doug Nelson, Chiron Inc, Emryville, California USA.

David Parsons, Sydney Water, Sydney.

Neil Porter, Department of Defence, Canberra,

Clare Sullivan, Emergency Management Australia, Canberra.

Mike Tarrant, Emergency Management Australia Institute, Mt Macedon.

Costa Zarkis, Marsh Pty Ltd, Sydney.

L A practitioners' guide to business continuity management Work book

The following blank templates are included in the Work book (template numbers refer to the worked examples within the respective Chapters of this Guide):

Commencement

Template 2.1: Identification of critical business functions

Risk and vulnerability analysis

Template 3.1: Disruption risk register

Template 3.2: Disruption scenario register

Business impact analysis

Template 4.1: Workload demand and variation

Template 4.2: Determining impacts on the business

Template 4.3: Determining resource requirements

Template 4.4: Determining responsibilities and operational activities

Template 4.5: Determining alternate workarounds

Template 4.6: Determining customer dependencies

Template 4.7: Determine supplier dependencies

BCM Strategy development

Template 5.1: Strategy development

Maintenance of BCM

Template 9.1: Exercise

Template 2.1
Example template for the identification of critical business functions

Critical business function or process	Physical location	Critical success factors	Functional interdependencies	Priority	Practical grouping

Template 3.1
Disruption risk register

Risk sources *(What are the potential causes and contributing factors)*	Risk *(Including detailed description of the risk)*	Overall disruption risk/ risk scenario	Risk assessment			Existing controls or strategies	Vulnerabilities	Treatments		Responsibility
			Consequence	Likelihood	Risk rating			Being developed	Need to be developed	

Template 3.2
Disruption scenario register

Overall disruption risk/ risk scenario *(Obtained from Column 3 of Risk & Vulnerability Register)*	**Location(s)** *(Where specific sites are involved)*	**Critical business function**	**Impact on business operations** *(Describe the overall impact to the successful operation of your business and the key business functions affected)*	**BCP status**	
				Current	**Required**

Template 4.1
Workload demand and variation

Critical business function	Critical dates																			Specific priority dates	Key contact person
	Month												Days								
	J	F	M	A	M	J	J	A	S	O	N	D	M	T	W	T	F	S	S		

Template 4.2
Determining impacts on the business

Critical business function	Impacts: Financial impacts (Rate 1 to 5)						Impacts: Non-financial impacts (Rate 1 to 5)						Highest Impact (Provide a description of the highest rated impact)	MAO (Maximum acceptable outage)	RTO (Recovery timeframe objective)	RPO (Backlog processing)
	<1 Hour	1 -4 Hours	1 Day	2 - 7 Days	1 - 4 Weeks	> 1 month	<1 Hour	1 -4 Hours	1 Day	2 - 7 Days	1 - 4 Weeks	> 1 month				

Template 4.3
Determining resource requirements

Minimum resource requirements								
Critical business function/process: invoice processing								
Resources	**Current resource level** *(available to complete key business process)*	**Resource requirements** *(Minimum levels required to complete key business process)*						**Manual alternate workarounds** *(Yes/ No)*
		<1 hour	**1 to 4 hours**	**1 Day**	**2 to 7 Days**	**1 to 4 weeks**	**> than 1 month**	

Template 4.4
Determining responsibilities and operational activities

Critical business function: issues management				
Person	**Position**	**Alternate or standby**	**Key responsibility/activity**	**Reports to**

Template 4.5
Determining alternate workarounds

Critical business function: market analysis			
Critical resource requirement	**What critical tasks/activities/processes can be performed**	**What critical tasks/activities/processes cannot be performed**	**What alternative processes or workarounds can be employed**

Template 4.6
Determining customer dependencies

Critical business function	Major customer/stakeholder	Key contacts – details	Minimum contracted or acceptable requirements	Alternate continuity arrangements

Template 4.7
Determine supplier dependencies

Critical business function: security threat assessment			
Contracted goods and services	**Minimum acceptable goods and services**	**Supplier contact details**	**Alternate supplier contact details**

Template 5.1
Strategy development

Organisational unit:	
Location:	
Contact name:	
Title:	
Telephone:	
Email:	

Critical business function			
Critical infrastructure			
Risk scenario			
MAO time		**RTO**	
Response requirements			
Response option 1		**CBA*:**	
Response option 2		**CBA:**	
Response option 3		**CBA:**	
Response option 4		**CBA:**	
Recommended option		**Response objectives**	
Detailed description of response			
Preparatory requirements			**Responsibility**

* CBA – Cost Benefit Analysis

Template 9.1
Exercise

Business unit:	
Location:	
Contact name and title:	
Telephone:	
Email:	

Exercise title							
Plans to be tested							
Critical business function/ organisational units involved							
Exercise location(s)		**Date (1)**		**Start time**		**End time**	
		Date (2)		**Start time**		**End time**	
		Date (3)		**Start time**		**End time**	
		Date (4)		**Start time**		**End time**	
Exercise objectives							
(1)							
(2)							
(3)							
Resources involved/required							
Exercise exclusions							
Support requirements							
Exercise facilitator			**Exercise approved by**				

NOTES

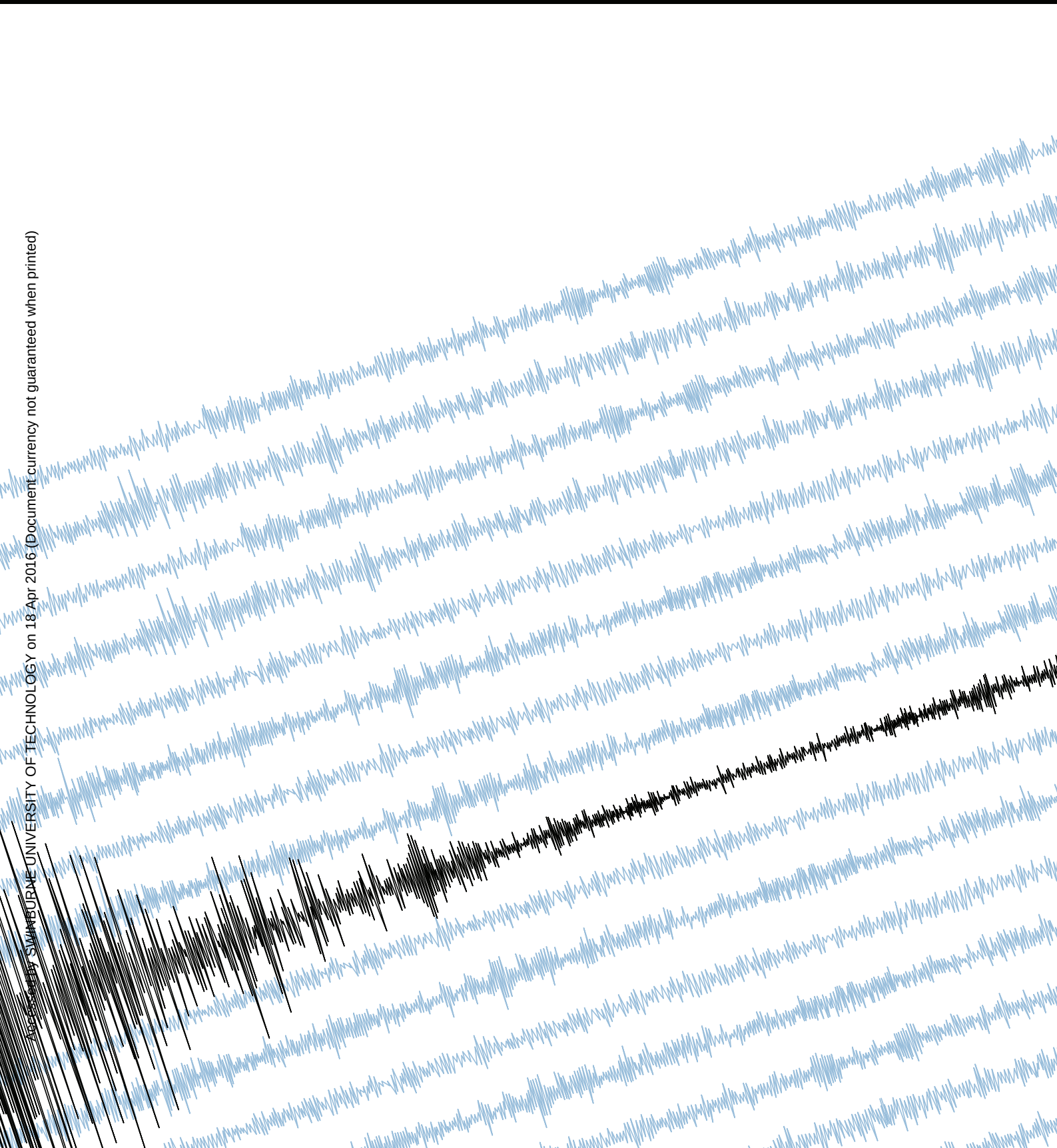
NOTES

NOTES

ISBN 0 7337 7472 5

Standards Development
Standards Australia
GPO Box 476
Sydney NSW 2001
Phone: 02 8206 6000
Fax: 02 8206 6001
Email: mail@standards.org.au
Internet: www.standards.org.au

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



This page has been left intentionally blank.