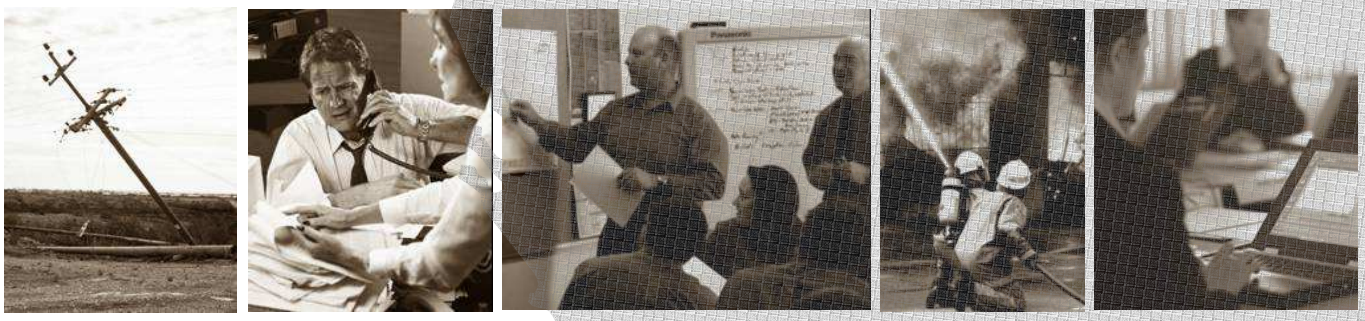
WESTERN AUSTRALIAN GOVERNMENT

BUSINESS CONTINUITY MANAGEMENT GUIDELINES

Third Edition



RiskCover

Acknowledgement

RiskCover *has produced the Business Continuity Management Guidelines to assist the Western Australian Government agencies to develop and implement their Business Continuity Plans.*

First edition August 2006
Second edition July 2009
Third edition June 2015

Please direct all enquiries or comments on the contents of this document to:

Insurance Commission of Western Australia
RiskCover Division
221 St George's Terrace
Perth Western Australia 6000
(08) 9264 3333

Table of Contents

LIST OF APPENDICES 28

IN BRIEF

These Guidelines are intended to be used by any Western Australian Government agency (agency) that is in the process of or intending to develop effective Business Continuity Management processes.

These Guidelines are presented in two parts:

Part One: An introduction to Business Continuity Management

Part Two: The Business Continuity Management Process

- Step 1 – Programme Management
- Step 2 – Risk and Business Impact Analysis
- Step 3 – Identification of Response Plan Options
- Step 4 – Development of Response Plans
- Step 5 – Train, Exercise and Maintain

These Guidelines are consistent with AS/NZS 4360 and HB 221:2003 with some modifications for Western Australian agencies.

These Guidelines should be used in conjunction with the Western Australian Government Risk Management Guidelines.

PART ONE: INTRODUCTION

The objective of Business Continuity Management (BCM) is to ensure the timely resumption and delivery of essential business activities in the event of a major disruption by maintaining the key business resources required to support delivery of those activities. The primary output of the BCM Process is a Business Continuity Plan (BCP), which is a plan for mitigating some of the agency's risks.

The BCP is initiated when a risk event occurs that has a business interruption consequence. The business interruptions that are of concern from a continuity viewpoint are referred to as 'outages'. These events will cause a significant disruption to, or loss of key business activities over a prolonged period of time. It follows that such events will have a high impact on and severe consequence for the agency.

Outages need to be distinguished from other day to day operational problems such as system glitches, brief loss of communications link and processing errors that arise from time to time in the normal course of doing business. These events should be handled as part of the businesses' standard operating procedures and typically do not come under the purview of the BCP.

The concept of an outage has a time dimension as well as a business impact dimension. The BCM Process includes establishing the maximum periods for which each business activity can be disrupted or lost altogether, before the potential business impacts (such as damage to reputation, financial loss, effects on stakeholders and breach of regulations) become unacceptable to the agency.

BCM focuses on consequences of an outage and the steps necessary to contain or minimise the negative consequences when an outage actually occurs. It is not concerned with the likelihood of occurrence, as matters of likelihood should already have been addressed as part of the RM process. Preventative controls should already have been established to reduce the likelihood and consequences of the risk event to levels that are acceptable to management.

Effective BCM goes beyond the construction of a BCP. It requires a fundamental cultural change within the agency, including an acceptance of uncertainty. People at all levels of the agency need to appreciate that risk is inherent in all decisions and activities and that a proportion of these risks have the potential to create interruption to services, and that they therefore need to consider how they will respond to and manage such interruptions.

Agencies may have different approaches to responding to and managing crises. Regardless of the approach, the key elements that can usually be distinguished and collectively make up a BCM response plans are:

***Emergency Response*:** The initial response to a disruption, which involves the protection of people and property from immediate harm. An initial reaction by the Crisis Management Team will form part of the agency's first response.

***Continuity Response*:** Processes, controls and resources are made available immediately following an interruption to ensure that the agency continues to deliver its critical business services.

***Recovery Response*:** Processes, resources and capabilities of the agency are re-established to return the agency to normal operations. This will often include the introduction of significant organisational improvements, even to the extent of re-focusing strategic or business objectives.

Business Continuity Management is in essence a management process focussed on what to do following an unexpected event or incident, which is best developed prior to an incident occurring, in the relative calm of daily management of the agency. Planning and making decisions on the run in the heat of a crisis situation is both difficult and dangerous.

Relationship between Business Continuity and Risk Management

Business continuity is an element within the wider context of Risk Management (RM). RM is the practice of systematically identifying, understanding and managing the risks encountered by an organisation. The RM Process is illustrated in Figure 1.

A structured, systematic approach to RM will enable agencies to develop a thorough understanding of the risk issues that may prevent the achievement of goals or objectives. As part of this process, the agency should define its essential functions and key dependencies, and also clearly identify those risks which may potentially result in an interruption to the services. A BCP is a means of minimising the impacts of a particular risk, however it is not a preventative control for all risks.

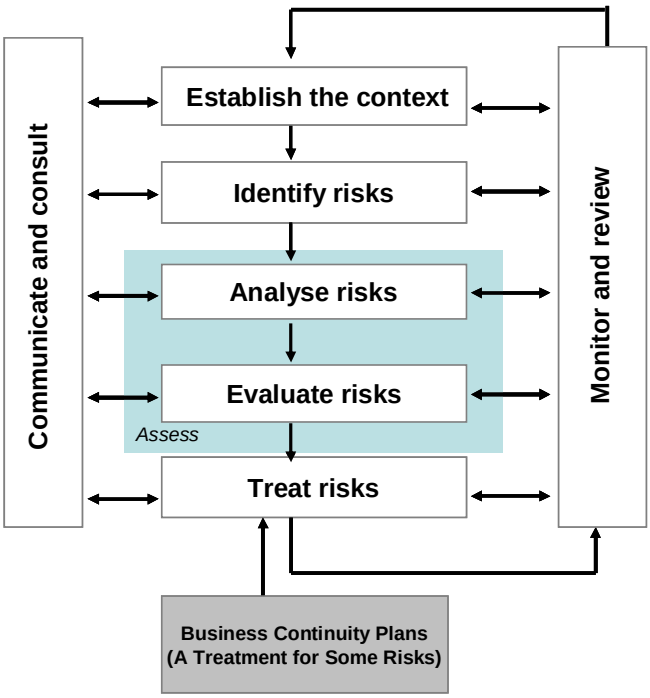


Figure 1 Risk Management Process (based on AS/NZS4360)

RM and BCM need to be considered as part of an integrated process. RM – the identification, analysis and evaluation of risks – is the important early step to understanding the risks and scoping the need for BCPs. The interface between RM and BCM is illustrated in Figure 2.

Further information relating to the Western Australian Government's RM approach can be found in the Western Australian Government Risk Management Guidelines.

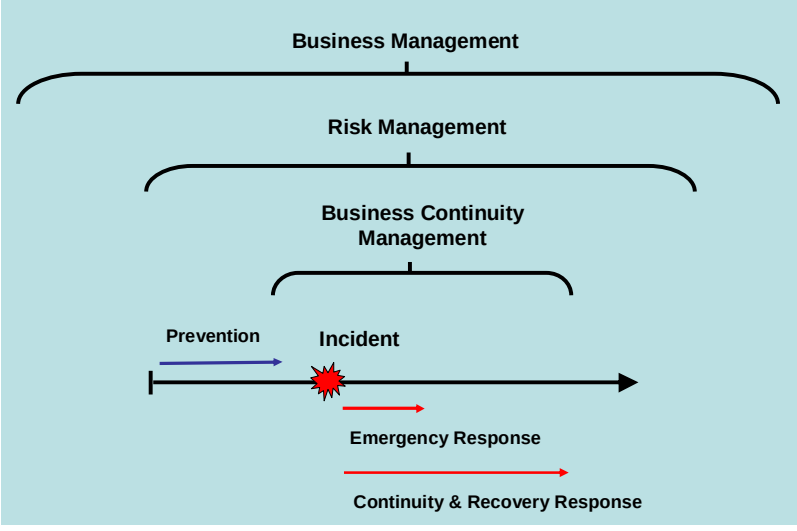


Figure 2 Risk Management and Business Continuity Management Interface

PART TWO: THE BUSINESS CONTINUITY MANAGEMENT PROCESS

1. OVERVIEW OF THE BUSINESS CONTINUITY MANAGEMENT PROCESS

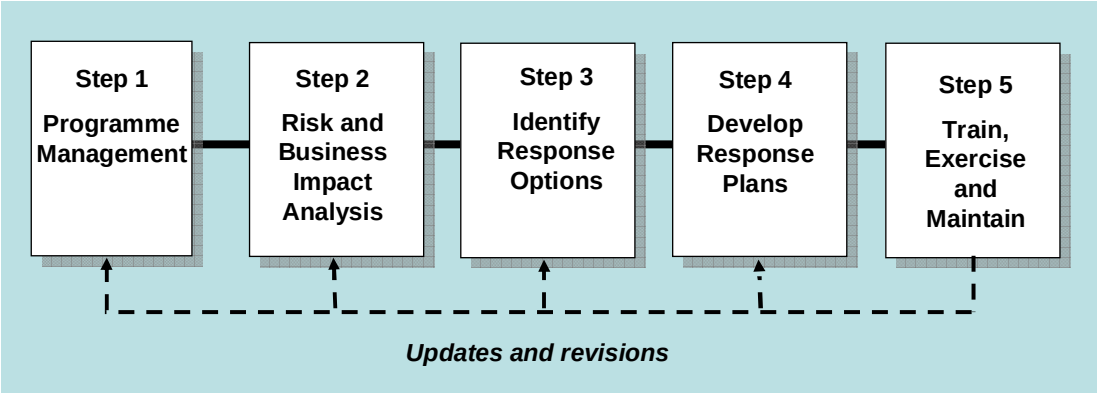


Figure 3 Business Continuity Management Process

Step 1 Programme Management

The primary focus of this step is obtaining Executive support and commitment of resources to develop and maintain the agency's BCM programme. As BCM is an integral part of an organisation's approach to managing risk, this should be completed as part of the development of an agency's overall RM programme. This would include the endorsement of the development and implementation of appropriate risk mitigation strategies, including BCPs, by the agency's Executive.

Step 2 Risk and Business Impact Analysis

The emphasis of this step is on prioritising the business activities that are critical and identifying the resources that are required to support these activities for business continuity purposes. This involves:

- identifying the business activities that are performed by the agency;
- assessing the potential business impact on the agency should these activities be interrupted over varying timeframes;
- determining the timeframes within which critical business activities must be resumed following an outage; and
- identifying the resource requirements for business continuity.

Reference should be made to the agency's operational RM programme, where in many cases, critical activities and risks to those activities may have already been defined.

Step 3 Identify Response Options

This step involves the identification and assessment of response options to meet the agency's requirements for business continuity, covering people, IT systems and networks, premises and facilities, and data backup and offsite storage. The recommended options, along with the associated budgets and implementation plans, are then presented for Executive approval.

Step 4 Develop Response Plan

Once the appropriate response option has been approved, the process of developing the response plan begins. This involves organizing managers and employees into crisis management and business continuity teams, developing processes for incident notification and escalation, and documenting business continuity action plans for critical business activities. This is also the time when any physical implementation work such as procurement of backup equipment and commissioning of alternate sites are carried out.

Step 5 Train, Exercise and Maintain

This is the step to ensure that what has been developed and documented will actually work to enable the agency to continue to deliver critical business activities when a crisis arises. This involves training relevant employees on the use of the plan, conducting exercises to validate the completeness and accuracy of the plan, and putting in place a schedule for the on-going maintenance of the plan.

The key components and deliverables in relation to each step of the BCM process are illustrated in Appendix 2.

2. STEP ONE: PROGRAMME MANAGEMENT

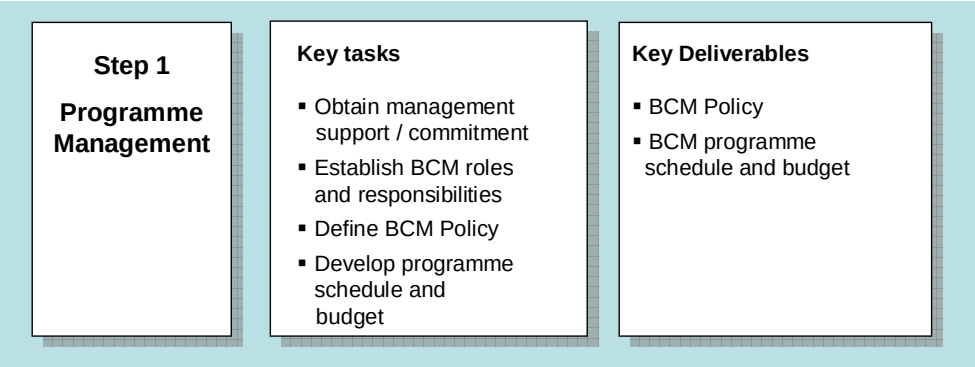


Figure 4 Step 1 Programme Management

2.1 Overview

Business Continuity Management should be an integral part of an agency's RM programme. As with RM, effective implementation is dependent upon leadership commitment and demonstrated support. This step is concerned with demonstrating Executive leadership through the development and communication of a BCM policy, the assigning of specific roles and responsibilities and the development of a programme schedule of how the BCM is to be implemented. Included in that schedule will be a clear definition of the objectives, scope, budget and deliverables associated with the programme, along with the required resources needed to support the programme.

2.2 Roles and Responsibilities

The Board/Executive Committee has a specific role in demonstrating commitment to the development and maintenance of the Business Continuity Plan, by showing leadership in the execution of the BCM programme. In order to facilitate this, an executive sponsor should be assigned the task of overseeing the implementation of the programme and the development and testing of the BCPs.

Every Senior Manager should have a defined responsibility for the implementation and management of BCM within their area(s) of responsibility.

In addition, there are a number of specific roles to be allocated, as listed below:

i) RM Steering Committee

The role of this committee is to provide Executive level oversight to the BCM programme. This committee should be made up of key senior executives representing the key business and support areas.

ii) BCM Programme Manager

The role of the BCM Programme Manager is to coordinate and support the agency in the development and implementation of its BCM programme. The manager is responsible for putting in place a BCM process and guiding the business and support areas through the process. This may be a full time role but more commonly, the role is often taken up by someone who is also responsible for coordinating RM.

iii) BCM Coordinators

BCM Coordinators are appointed within each division or department. Their key role is to act as a single point of contact for all BCM issues and to ensure that BCM activities are carried out within their divisions or departments under the guidance of the agency's BCM Programme Manager.

A sample terms of reference for the above roles is presented in Appendix 3.

2.3 BCM Policy

A BCM Policy outlines the principles and context of what BCM is to the agency and how the agency will act in relation to BCM. It helps to communicate and reinforce the message that the Executive is committed and serious about BCM.

As business continuity needs to be integrated as part of RM, it is important that the policy on BCM be developed in conjunction with the agency's overall RM framework. Ideally, BCM should be addressed within the agency's Risk Management policy. However, should this not be practicable, care should be taken when drafting a separate policy for BCM that it is done within the context of RM.

A sample table of contents for a BCM policy is presented in Appendix 4.

2.4 Develop BCM Programme Schedule and Budget

A BCM programme schedule defines the tasks needed to develop, implement, test and maintain the agency's BCPs, the people responsible for carrying out the tasks and the expected timeframe to complete the tasks. This provides a road map for navigating through the BCM process and a means for monitoring status, and is part of any good project management discipline.

A sample BCM programme schedule is presented in Appendix 5.

HINTS:

- *In some instances, it may also be necessary to supplement the programme schedule with the resource requirements and budget needed to support the programme. This may include project management costs, time costs for staff to attend interviews, workshops and exercises, professional fees if outside help is needed, as well as incidental costs for office supplies and project administrative support. At this stage, the requirements and costs are associated with carrying out the BCM process and NOT with the implementation of specific response strategies (such as backup systems and alternate sites) which will only be worked out in Step 4.*

3. STEP TWO: RISK AND BUSINESS IMPACT ANALYSIS

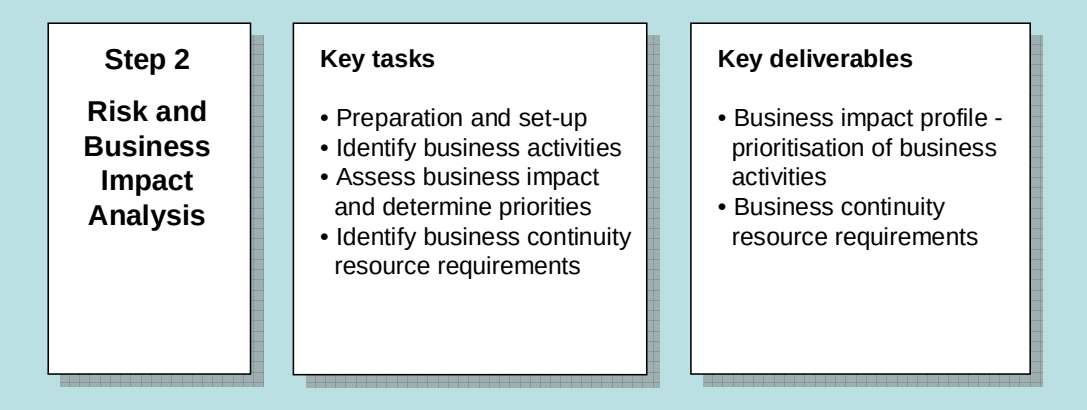


Figure 5 Step 2 Risk and Business Impact Analysis

3.1 Overview

When preparing for a Business Impact Analysis (BIA), it is important that Management has a clear understanding of the agency's business objectives, business activities and the critical success factors (key dependencies). Generally, this information is compiled as part of a structured risk assessment process and would include:

- the activities of the agency;
- the Critical Success Factors for each of the business activities;
- an assessment of risk associated with each of the business activities; and
- the treatments for unacceptable risks.

Risk treatment involves identifying a range of options to reduce the consequences and / or likelihood of an unacceptable risk. Amongst all the options, BCP is specifically a treatment for risks that could potentially interrupt business operations and cause unacceptable consequences to the agency.

The BIA builds on this information and takes the analysis one step further to determine the timeframes within which activities of the agency must be resumed following an outage. These timeframes are then used to prioritise activities that are critical for business continuity purposes.

If a structured risk assessment has not been undertaken by the agency, it is recommended that this is done before proceeding with the BIA. It is important that before proceeding to the BIA that the agency's risk profile is renewed and understood.

Further information relating to RM can be found in the Western Australian Government Risk Management Guidelines.

3.2 Approach to Business Impact Analysis

The BIA is an essential starting point for developing the BCP as it establishes the business requirements for the plan. The subsequent two steps in the BCM process, Identify Response Options and Develop Response Plan, are driven by the outcomes of the BIA. Get the BIA wrong and the chances are that the plan which is eventually developed will not fully cater to the business continuity requirements of the agency.

Assessing the potential business impact of an outage on an agency is inherently subjective in nature. The BIA process attempts to reduce the subjectivity by providing a consistent set of rules and measurement criteria that is applied across the agency. It is essential to get informed, objective and complete input during this step of the BCM process. Accordingly, the communication and consultation that are part of the RM process are particularly important here. Before starting, identify the appropriate parties for involvement and confirm their availability.

The key tasks in carrying out the Business Impact Analysis are:

i. Preparation and Set-up

The main tools used are the Business Impact Reference Table and BIA template. The purpose of the Business Impact Reference Table is to provide consistent definitions to different types of impacts and severity levels. Typically, impact types would include financial loss, reputation and image damage, stakeholder impact and regulatory / statutory violations. Severity levels could range from 1 (being insignificant impact) through to 5 (being catastrophic impact).

In preparing the Business Impact Reference Table, it is important that the definitions and severity levels used are consistent with the agency's Risk Reference Tables. If a structured risk assessment has already been carried out, the definitions and severity levels should already have been captured, and should be used for the BIA.

A sample Risk / Business Impact Reference Table is presented in Appendix 6A.

The BIA template is used to capture impact information for each activity assessed along two dimensions – severity (as defined in the Business Impact Reference Table) and duration of outage. In preparing the BIA template, it is important that the time windows used to define the duration of outage are relevant to the nature of the agency's activities. Typically, time windows of 1 day, 3 days, 5 days and 10 days are used.

A sample Business Impact Analysis template is presented in Appendix 6B.

ii. Identify Business Activities

This task starts by considering the agency's mission and deliverables and deciding what outcomes are essential for the achievement of the agency's business objectives. Once these essential outcomes are understood, it is possible to identify the business activities that are required to produce them. The functional organisational chart could also be reviewed to identify general areas of operational responsibilities and the activities that go along with these responsibilities. This step requires the Executive to take a whole of agency perspective and identify the agency's business activities.

A sample list of business activities is presented in Appendix 6C.

iii. Assess Business Impact and Determine Priorities

Each business activity identified is now subjected to the analysis using the BIA template and Business Impact Reference Table. The aim of the analysis is to determine the Maximum Acceptable Outage (MAO) of each activity – i.e. how long can an activity be disrupted before the consequences became unacceptable to the agency.

It is essential that inputs from senior management be obtained as the analysis needs to take a high level perspective of the likely impacts of an outage to the agency as a whole. It is often beneficial to conduct the analysis in a group workshop setting with senior managers across different areas so that different viewpoints could be considered. This would also provide checks and balances to keep the analysis as objective as possible, to what is otherwise a rather subjective process.

Refer to Appendix 6D and 6E for samples of the BIA.

When the MAOs for all the activities have been identified, a consolidated business impact profile can be developed for the agency. This profile essentially separates the activities into 2 main groups:

- time critical activities, i.e. those that must be operational within the BIA time windows; and
- non-time critical activities, i.e. those that fall outside the BIA time window and are thus not critical for business continuity purposes.

The key output of this step is a list of the critical business activities.

A sample consolidated business impact profile is presented in Appendix 6F.

It is essential that the consolidated business impact profile be presented and endorsed by the Executive at this stage as the profile provides the basis upon which the agency would develop its business continuity strategies and plans. The profile can be revised by the Executive should there be any contention but such actions should be minuted so that there is a proper audit trail.

iv. Identify Business Continuity Requirements (Resource Requirements)

Once the business impact profile has been endorsed by the Executive, the next task is to define the minimum resource requirements for business continuity. This involves identifying broad strategies, key dependencies and resources (people, IT systems and networks, premises and facilities, and data backup and offsite storage) needed to support the resumption of critical business activities within the required MAO timeframes.

Refer to Appendix 6G for a sample of how business continuity requirements can be tabulated.

HINTS:

- *This step in the process requires the gathering of information. This is best done through interviews or facilitated workshops. Information sought through questionnaires and email will be much less useful and timely than that which is obtained through personal contact.*

- *Remember the importance of communication and consultation. In particular, consult with your external stakeholders; they can provide valuable insight on expectations, outcomes, activities, and MAOs.*

- *Capture the information. It is important that everything is documented to proceed to the next step. Documentation also facilitates the monitoring and review of these underlying determinations upon which the BCP will be based.*

- *Not all of your resources will be required immediately. It is much more operationally efficient and cost effective to receive resources only as you need them. This is especially true of personnel; ensure you do not have excess people with no assigned duties during the initial stages of your recovery process. The MAOs for the identified critical activities will guide you in the timing of your resource requirements.*

- *Executive support and input is essential during this step (and every other step) of the BCM process. In particular, Executive should sign off on the critical activities and MAOs before proceeding to Step 3.*

4. STEP THREE: IDENTIFY RESPONSE OPTIONS

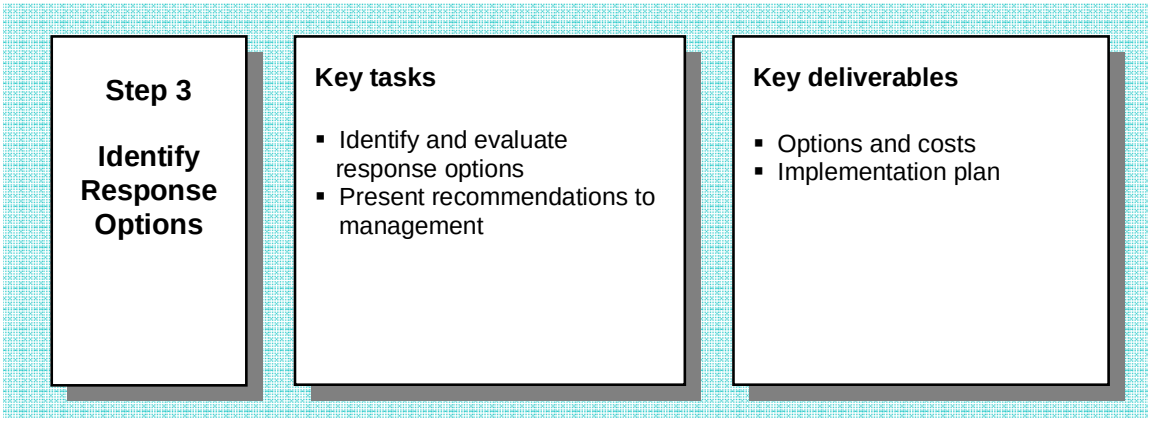


Figure 6 Step 3 Identify Response Options

4.1 Overview

At the end of Step 2 you will have identified; (a) the list of critical business activities, (b) the timeframe within which each of these critical business activities must be resumed following a disaster (i.e. the maximum acceptable outage (MAO), and (c) the resources that must be made available to support the resumption of these critical activities. This output is now used in Step 3 to formulate a set of response options that will meet the requirements for business continuity.

Response options may include temporarily suspending the activity, transferring the activity to an alternative organisation or individual, or relocating the activity to an alternate location. The fundamental principle behind the development of response options is that the shorter the MAO, the higher the investment will have to be on the business continuity solution since more resources will have to be placed on a "hot stand-by" basis. The cost / benefit of each option needs to be assessed against the requirements for business continuity. Recommendations on the most appropriate solutions should then be presented to the Executive for approval.

4.2 Identify response options

The key resources required to support business recovery encompass people, equipment, data, premises, services and supplies. In identifying response options, it is important to consider the quantity and timeframes within which these resources must be made available before, during and after an incident. Whilst having a dedicated, fully equipped and state-of-the-art backup facility that can be invoked at a moment's notice may be desirable, this may not be appropriate as the costs may far overweigh the risk / impact reduction benefits that can be derived from such an approach. Keep in mind that the immediate objective of business continuity is to ensure the resumption of critical activities within an acceptable timeframe and not necessarily business as usual.

There are four broad categories of response options:

i. Temporarily suspending the activity

Activities that are non-essential or are not required to be performed immediately following an incident may be suspended temporarily. At some point, these activities will nonetheless need to be resumed, but suspending them in the short term will allow you to free up resources for more critical tasks.

ii. Transferring the activity

Where the same activities are performed in different locations (such as regional offices), the work at an affected location may be passed over to the other non-affected locations. Some additional resources may be required to pick up the increased workload at other locations but little upfront investment is needed to implement this response option. This option has the benefit of leveraging on existing resources and infrastructure to provide reciprocal business continuity capability across the agency's network.

iii. Working from home

This response option would be viable for activities that have little or no dependency on the infrastructure of a normal office environment, and where face-to-face interactions with others are not essential. Typically, all the staff need is a notebook computer or home PC with remote access to the agency's system in order to work from home. However, always verify that the use of this option does not violate any guidelines, compliance requirements or legislation related to confidentiality of information, risk control measures, information privacy, security, and so on. In some agencies, this may not be an option as the services they deliver require specialised equipment or facilities.

iv. Relocating to an alternate (backup) site

An alternate or backup site is a facility that is appropriately equipped with the resources needed to support the resumption of critical services in the event the primary location is impacted by a disaster. The site may be one that is fully dedicated and equipped for business continuity only, and may have all the necessary office equipment, PCs, systems, and telecommunications capability on hot stand-by that can be activated within one or two hours.

Backup sites can also be created by converting existing facilities in other buildings for use in a disaster. Training centres, conference rooms and even cafeterias may be turned into recovery centres when needed. Some lead-time may be needed to reconfigure the layout and to install equipment but this can be a cost-effective means to provide recovery capability for activities that do not have very short MAOs.

The following need to be taken into account when considering response options:

i. People

- How does the agency minimize the risk of loss of key personnel?
- What is the agency's current Human Resources policy and practices on succession planning, cross training, job rotation, knowledge retention, resignation and retirement?

ii. IT systems and networks

- What is the agency's current IT disaster recovery capability? Does the agency have an up-to-date and workable IT disaster recovery plan?
- What IT resources will be required to support the response options and how will these resources be made available?
- Are any of the agency's IT systems and networks dependent on external service providers or shared services arrangements? What implications do these have on the response options and how should the implications be dealt with?

iii. Premises and facilities

- How much space and what types of facilities will be required to support the response options, and how will these be made available?
- What are the most practical and cost effective ways to provide for premises and facilities?
- How far away does the alternate facility have to be from the primary location?

iv. Data backup and off-site storage

- What is the agency's current policy and practices on data (both paper and electronic media) protection, retention, storage and restoration? Are these adequate and what needs to be done to close any gaps?
- What data is required for business continuity and how quickly does it have to be made available?

4.3 Evaluate response options

When evaluating each of the response options, it is necessary to consider the technical, operational and financial viability of each.

Technical viability refers to whether the option is able to fulfil the business continuity specifications and requirements of the critical activities – i.e. can the option meet the timeframe within which the activity must be resumed?

Operational viability refers to whether the option can realistically be implemented. For example, working from home may be technically feasible for someone performing an accounting activity but operationally may be prevented from doing so due to compliance requirements.

Financial viability refers to the cost to implement the option. Typically, this would include any capital or up front expenditure needed to set-up the option, plus running or recurrent costs for the on-going upkeep of the option.

Based on the evaluation, a recommendation should be presented to the Executive for approval.

HINTS:

- *When considering options for alternate sites, do not forget to look into the possibility of leveraging the available facilities across different agencies. For example, the same alternate site could be shared by a number of different agencies, or a reciprocal arrangement could be worked out between two agencies to make use of each other's office premises for recovery purposes. Doing so will save considerable costs for all concerned.*

- *This is the stage where the project is likely to stall if not managed carefully, as important budget decisions need to be made. Allow time to present the options and recommendations well ahead of the annual budget cycle so that the numbers can be incorporated into the agency's overall budget plan.*

- *Look for cost effective and pragmatic solutions. It is always difficult to justify spending on a dedicated, hot stand-by recovery site, which is left unused 99.9% of the time. Look for ways to make use of existing facilities. Collaborate with other agencies whenever possible.*

.

5. STEP FOUR: DEVELOP RESPONSE PLANS

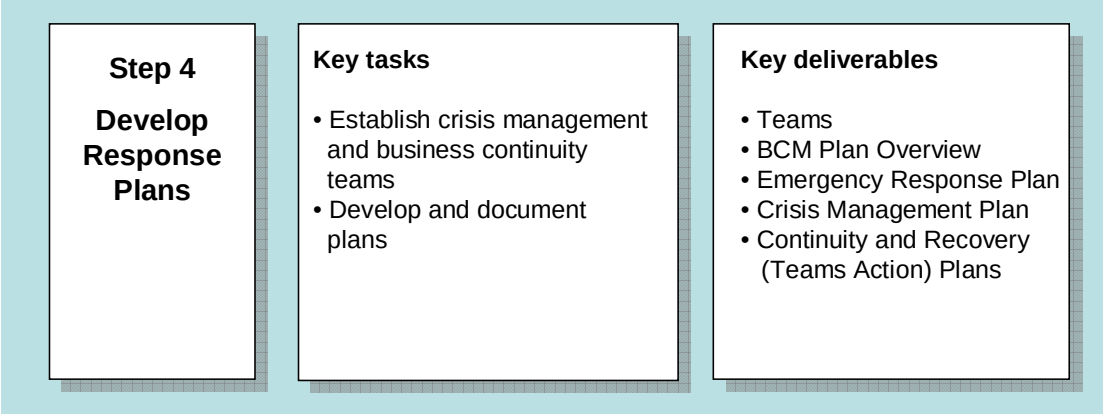


Figure 7 Step 4 Develop Response Plans

5.1 Overview

Having identified and selected the response options in Step 3, this step involves putting together the action-level processes and procedures necessary for the execution of these response options when an incident occurs. These include the agency's Emergency response, Continuity response and Recovery response. This is also the step where roles and responsibilities of crisis management and business continuity teams are specified and individuals assigned to these teams.

5.2 Establishing the Crisis Management and Business Continuity Teams

i) Crisis Management Team

The Crisis Management Team comprises of a selected group of key senior managers who are empowered and authorised to provide corporate leadership and direct business continuity activities at times of crises or emergencies. The team should be kept relatively small (no more than 10 to 12 people) to facilitate decision-making and would typically consist of the following roles:

- Crisis Manager
- Command Centre Coordinator
- Corporate Communications
- Human Resources
- Corporate Security
- Administration and Logistics
- Premises and Facilities
- Business Continuity Coordination
- IT Recovery Coordinator

In addition to providing leadership and direction during a crisis, these roles also provide important support to the business continuity and recovery efforts such as looking after staff welfare, communicating with the media, liaising with the civil authorities, and arranging transportation to the backup site. It is thus necessary that the roles and responsibilities as well as actions to be taken by each of the respective functions be documented as part of the Crisis Management Plan.

A sample terms of reference for the Crisis Management Team is presented in Appendix 7A

ii) Business Continuity Teams

Business Continuity Teams comprise of personnel who will be responsible to execute the continuity and recovery response plans when they are invoked. The number of teams required depends on the size of the agency but this should reflect the existing organisational structure of the agency. A team may represent a single department in the agency, or sub-teams, each with specialised functions, may be set-up for a larger and more complex department.

Each team should be lead by a Team Leader who has the responsibility to ensure that critical business activities within his / her department are resumed in a timely manner. It is also essential that an Alternate Team Leader be appointed as a backup to the Team Leader. Team members should be assigned to the team based on their relevance to the functions to be resumed. It is not essential for all personnel in a department to be in the team.

A sample terms of reference for Business Continuity Teams is presented in Appendix 7B.

5.3 Develop and Document Plans

It is necessary to document the business continuity plan as it serves as a reference for people to act in a certain way that is consistent with approved strategies of the agency in the event of a major incident. However, one needs to keep in mind that a plan document is not a complete, step-by-step, how-to-do-it manual since each incident is unique, with varying levels of threats and business impact. As such, a pragmatic approach should be taken on documentation. Keep the plans simple and easy to follow – more pages do not necessarily mean a better plan.

As a general guideline, always separate background information that is not required for responding to an incident from the information that is needed to guide decision making and actions when an incident occurs. The documentation can be broken down into the following component plans:

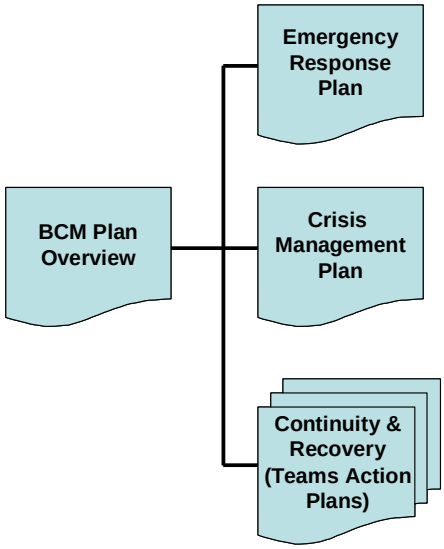


Figure 8 Components of BCM Plan Documentation

i) BCM Plan Overview

The BCM Plan Overview is designed to provide a high level description of the framework, policy, processes and broad strategies that make up the agency's BCM programme. Such information is not required for guiding decisions and actions during an incident but is nonetheless important for the purpose of providing evidence of an agency's BCM programme. Typically the information presented would include an overview of the BCM process, BIA findings, business continuity strategies and requirements, response options considered, and testing, training and maintenance protocols.

A sample table of contents of a BCM Plan Overview document is presented in Appendix 8A.

ii) Emergency Response

(a) Emergency Response Plan

An Emergency Response Plan is designed to be invoked immediately following a critical incident for the protection of people and assets. Typically, the plan would cover:

- instructions on actions to be taken by staff during an emergency such as bomb threat, fire, explosion and flooding;
- instructions on how to evacuate the building, location of muster points and process for accounting for staff;
- names of floor wardens, and their roles and responsibilities; and
- emergency contact numbers that staff should call to report an incident or to obtain information.

Most agencies would already have some aspects of such plans in place. These would usually come under the responsibility of the security, building management or occupational safety and health area of the agency. As such, it is important that the BCM Programme Manager works closely with these groups to incorporate emergency response planning into the agency's overall BCM programme.

A sample table of contents for an emergency response plan is presented in Appendix 8B.

(b) Crisis Management Plan

A Crisis Management Plan sets out the principles to be followed should any incident cause, or threaten to cause, serious business impact on the agency. The plan provides a process that facilitates organised decision making on critical issues to cope with any serious incidents that might otherwise be quite chaotic. The plan is designed to be used by the Crisis Management Team (described in section 5.2), and consists of the following key components:

- guidelines to define what constitute a crisis and the triggers for activating the plan;
- roles and responsibilities of teams and individuals;
- processes for notification, escalation, mobilisation and de-escalation;
- considerations for dealing with operational and strategic implications;
- protocols and processes to ensure effective internal and external communications;
- consideration and processes for providing employees' assistance; and
- data collection and event tracking logs.

A sample table of reference for a Crisis Management Plan is presented in Appendix 8C.

iii) Continuity and Recovery Response (Teams Action Plans)

The Continuity and Recovery Response Plan (or Team Action Plan) is focused on individual business continuity teams. It is designed to provide team level response to maintain critical business activities following a major incident and to recover from the incident in order to return to normal operations.

Continuity procedures operationalise the response options identified in Step 3 for the resumption and continuity of critical business activities within the required maximum acceptable outage (MAO). These procedures should encompass all instructions necessary to guide the staff on plan execution and provide answers to a number of fundamental questions such as *" Who do I call?", "Where do I go?", "What needs to done?", "When do I have to do it?", and "What resources do I need?"*

Recovery procedures are directed towards restoring full operational capability and returning to business-as-usual after the crisis is over. The principle purpose of recovery response is the staged return to a level of normal (pre-disruption) capability and performance. Depending on the nature of the incident, recovery response may be completed quickly if there has not been any damage to physical infrastructure (for example, staff may return to the office to resume normal operations immediately after the "all clear" has been given following a bomb threat) or may run into weeks or even months after a major catastrophe (as experienced by some firms during 9/11 that took over 6 to 9 months to fully recover).

IT will also have its own action plan (typically referred to as an IT Disaster Recovery Plan) that sets out the technical procedures for the restoration and recovery of IT services. This plan outlines the process for notifying and mobilising IT resources, the timeframes within which IT services required to support critical business activities must be resumed, and steps for restoring systems, applications, data and telecommunications at the agency's backup (disaster recovery) facility.

The Continuity and Recovery Response Plan document will vary between agencies in terms of content and components, and will have varying levels of detail depending on the complexity of the solutions and culture of the agency. The documentation should be 'action orientated' but kept simple and flexible so that it can easily be referenced during an incident. Information that is not required to be used in an emergency (such as plan testing and maintenance procedures) should be documented separately.

A sample template of a Continuity and Recovery Response Team Action Plan is presented in Appendix 8D.

HINTS:

- *When documenting the response plans, keep the language simple and succinct so that the plan can be followed easily during an emergency.*

- *The plans should be modular, so that specific elements of the plan (e.g. Human Resources or IT) can be actioned independently by the appropriate part of the team.*

- *The plans need to strike the right balance between being prescriptive and being flexible. On one hand, they must provide clear direction for stressful and demanding circumstances. However, there is no way to know in advance exactly what those circumstances will be or how they will unfold. The plans must be able to adapt.*

- *The people who would be using the plan during an incident should participate in the development of the plan. This is to ensure that inputs to the plans are provided by the appropriate practitioners and that you do not end up with a theoretical plan.*

- *Each of the plans has a number of key roles, which need to be defined with designated substitutes. It is useful to assign these roles by position rather than individual, with a current table or chart to show who occupies what position. This reduces the burden of updating the plan as people rotate through different jobs.*

- *Information Technology (IT) is an essential part of every agency's operation, and detailed treatments for IT continuity and recovery are a key aspect of BCM. However, IT is only one part of business continuity. Ensure the IT plans integrate with the overall plan and that other critical activities are not undervalued because of an overemphasis on IT.*

- *It is important to review all plans as an integrated suite, ensuring that information flows, response actions are logical, consistent and collaborative and that resource allocation and use is efficient, effective and achievable.*

6. STEP FIVE: TRAIN, EXERCISE AND MAINTAIN

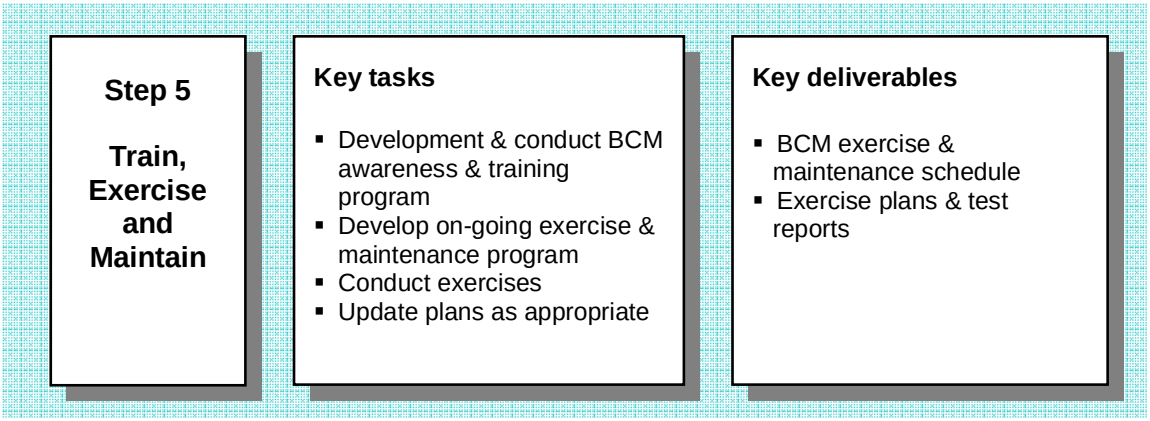


Figure 9 Step 5 Train, Exercise and Maintain

6.1 Overview

Step 5 brings the planning process to a logical conclusion and also sets up a process to ensure that the plan continues to be relevant to the agency on an on-going basis. This involves; (a) training the staff on how and when the plan is the be used, (b) exercising or rehearsing the plan to ensure that staff are indeed able to execute the plan, and (c) putting in place a maintenance process to keep the plan current and relevant.

6.2 Training

To ensure that BCM capability continues to reflect the nature, scale and complexity of the agency it supports, it must be understood by all staff and stakeholders. The primary objective of training is to ensure that the importance of BCM is understood by all staff in the agency and they are aware of their roles and responsibilities during an emergency or crisis situation.

Training may be pitched at different levels of the organisation, depending on what the needs and objectives are. Typically, these may take the following forms:

- General staff awareness training – delivered to all staff and may be incorporated into the inductions programme for new hires. This may cover topics such as; (a) an overview of what BCM is, (b) why is BCM important to the organisations, (c) what is the staff's role in an emergency, (d) what should the staff do if the BCM plan is invoked, and (e) what are the emergency contact numbers.

- BCM Coordinators training – delivered to staff with specific BCM responsibilities within their own departments. The aim is to improve the BCM skills of the coordinators as well as to help build ownership of the BCM process within the departments. Key topics may include; (a) BCM concepts, processes, corporate recovery policies and objectives, (b) how to complete/update risk / impact assessments, (c) how to document recovery plans, and (d) how to test the plans.

- Senior management training – delivered to senior managers of the agency with the aim of providing a strategic view of how the BCM programme is linked to the agency's mission and objectives. Such training is also a good vehicle for getting senior level buy-in and support for the BCM programme.

6.3 Exercising

A business continuity plan is of little use until it can be validated that it is actually workable in the event of a business interruption. This can be achieved by 3 steps - exercise, exercise and exercise:

Exercising the plan helps to:

- ensure the components of the plans are complete and current;
- provide comprehensive practice for staff involved in recovery activities;
- to ensure awareness of key suppliers and partners of the agency's reliance on them in the event of a plan invocation;
- identify where recovery processes failed and the actions and costs required to resolve; and
- satisfy auditors and insurers with documented and tested plans.

Exercising of the business continuity plan may be staged in the following manner:

- Component – where only a single process or component of the plan is exercised. Such an exercise is less formal and may be conducted more frequently. Examples are activation of the call out list, recall of backup tapes from off-site storage and recovery of a single business process.

- Integrated – where a number of inter-related components are exercised concurrently to validate that they can work together to complete the required objective. Such exercises require some planning and coordination. An example would be to a call out test combined with mobilisation of staff to the backup site.

- Full – involves exercising the business continuity plan in its totality to ensure that every aspect of it is working. Such an exercise will require extensive planning, coordination and cooperation across the agency. It is advisable that a full exercise should only be attempted after extensive component and integrated exercises.

There are also differing methods of exercising depending on what the scope and objectives are and what resources are available to support the exercise. These include:

- desk check – where the plan is validated against a checklist to ensure that standards and requirements are met;

- walkthrough – where business continuity team members verbally go through and discuss how they would handle an incident based on what has been documented in their plans; this allows the team to confirm the plan's effectiveness and identify gaps, bottlenecks or other weaknesses that need to be fixed;

- table top – where the team is presented with a predefined scenario and participants role play with simulated responses and act out the critical steps; such exercises are primarily targeted at the Crisis Management Team to help foster team interaction and decision making, and to validate specific response capability;

- simulation – where business continuity teams are required to carry out certain business continuity activities in a simulated environment under conditions that would exist in the event of an actual plan activation; and

- live exercise – where teams have to execute their business continuity plans in a live environment during operational hours.

An Exercise Plan should be prepared and approved by management prior to any major exercises. The Exercise Plan outlines the objectives and scope of the exercise, roles and responsibilities, assumptions and parameters, criteria for assessing the outcomes, and logistics aspects of the exercise, such as date, time, venue, transportation, and technical support.

De-briefing should be conducted immediately after each exercise to identify lessons learned and ways for improving the exercise and / or business continuity plans. An Exercise Report outlining the outcomes of the exercise, lessons learned and recommendations for improvements should also be prepared and presented to management for endorsement.

6.4 Maintenance

Having a plan that is out-dated is as good as not having a plan at all. A maintenance programme ensures that the business continuity plan remains current and relevant, ready to handle any crisis despite the constant change and dynamic environment that all organisations experience. It should be viewed as part of normal change management processes rather than be a separate structure.

The frequency of maintenance is dependent on the nature of the agency's business and the dynamism of the business environment in which the agency operates. Maintenance will likely need to be undertaken:

- when new processes are added or existing processes are modified or removed;
- when there is a major change to the agency's technology or location;
- after the agency has performed an exercise;
- after an audit where gaps have been identified and recommendations for improvements made; and
- in accordance with the agency's BCM maintenance programme.

When developing a maintenance programme, the timeframes within which different components of the business continuity plan need to be reviewed and updated should be specified. For example:

Plan component	Maintenance timeframe
BCM Policy	Reviewed and updated bi-annually
Business Impact Analysis	Reviewed and updated once a year or when there are any significant changes to the business
Business Continuity Plan	Reviewed and updated once a year, when there are any significant changes to the business, and immediately after any exercises
Contact Lists	Reviewed and updated every 3 months

From time to time, it would also be beneficial to conduct an impartial review / audit of the BCM programme against established standards and good practices. Such a review would provide independent assessment on the agency's existing BCM competence and capability, and provide assurance that the plans meet the required standards and are fit for purpose.

A sample BCM plan review checklist is presented in Appendix 9.

LIST OF APPENDICES

Appendix 1 Glossary of BCM Terms

Business Continuity Management (BCM)

Business Continuity Management is a discipline that prepares an organisation for the unexpected. It is a management process that provides the framework for building resilience to business and service interruption risks, responding in a timely and effective manner to ensure continuity of critical business activities, and ensuring the long term viability of the organisation following a disruptive event.

Business Continuity Plan (BCP)

The principle output of the BCM process. A BCP is, in effect, a treatment plan for certain risks, the consequences of which could disrupt core functions. The plan outlines the actions to be taken and resources to be used before, during and after a disruptive event to ensure the timely resumption of critical business activities and long term recovery of the organisation.

Business Impact Analysis (BIA)

The process of assessing the potential consequences to an organisation of an outage to its key business activities over varying periods of time, and prioritising the timeframes in which these activities must be resumed following a disruptive event.

Consequence

The impact or outcome of a risk eventuating. A risk can have multiple consequences.

Consequence Categories

These are key impact areas, which if affected as a result of a particular risk event, could have a significant impact on the ability of an agency to deliver its outcomes. Consequence Categories are agency specific, and should reflect the agency's economic, social and environmental responsibilities.

Critical Success Factors (CSF)

A factor which is essential for the successful performance of a key business activity.

Disaster Recovery Plan (DRP)

The policies, processes and procedures related to preparing for the recovery and restoration of information technology infrastructure required to support critical business activities following an outage of an organisation's computer centre. The disaster recovery planning process is a subset of BCM. The term disaster recovery is not to be confused with that used in the context of community emergency management which refers to it as a phase within the emergency management process that is concerned with actions related to rebuilding destroyed or damaged property, re-employment and restoration of essential infrastructure following a disaster.

Key Business Activities

Any high level activity or function that is instrumental in an agency delivering required outcomes or performing its mission.

Key Dependency

Relationship with or reliance upon another party essential to delivering outcomes or services. Key dependencies can be within the agency or external.

Maximum Acceptable Outage (MAO)

The maximum length of time that a key business activity may be suspended following an outage before the consequences will have a detrimental effect on the organisation.

Outage

An outage is an extraordinary natural or human-induced event, causing a disruption to, or loss of, key business activities, which has a significant impact on the organisation. This is distinct from minor interruption of services such as system glitches, processing errors and brief loss of communication links that may occur as a part of normal operations where it does not cause any significant impacts on the organisation.

Risk (or Risk Event)

"The effect of uncertainty on objectives" (from ISO 31000:2009).

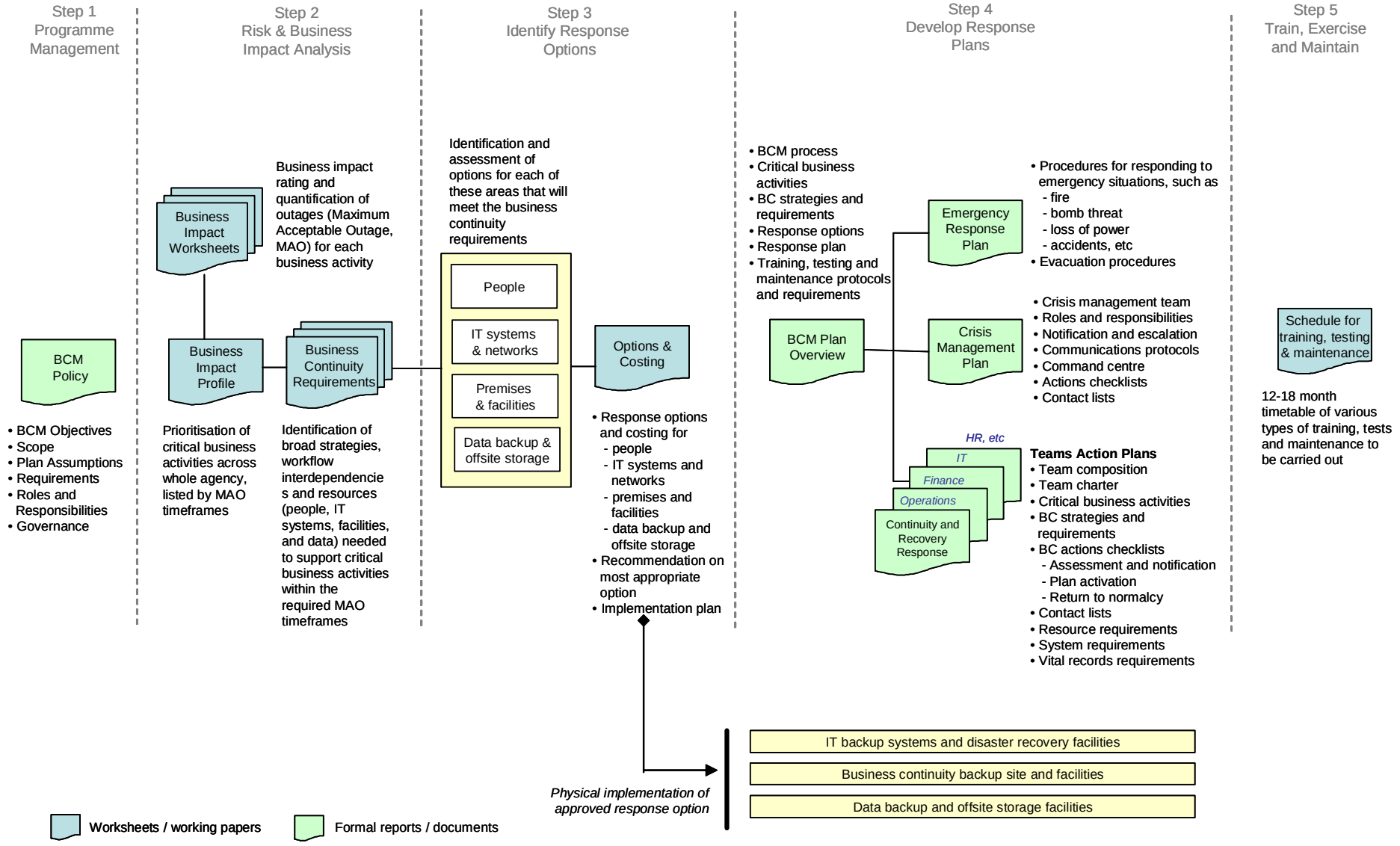
Risk Management

The practice of systematically identifying, understanding, and managing the risks encountered by an organisation.

Risk Management Process

The process of implementing, maintaining and embedding RM in an organisation, as set out in these Guidelines. The process consists of four sequential steps plus the overarching processes of Communication & Consultation and Monitor & Review.

Appendix 2 Key Components of Business Continuity Management



Appendix 3 Sample Terms of Reference

RISK MANAGEMENT STEERING COMMITTEE

The Risk Management Steering Committee provides senior management oversight to the business continuity management programme. It will:

- ensure that adequate business continuity plans are prepared, funded, tested and that decision making authority in the event of a crisis is clearly defined;
- approve the agency's BCM strategy and plans;
- monitor divisional compliance with the agency's BCM policy, strategy and requirements; and
- report status and highlight major issues to the Executive and Board.

Membership is made up of senior executives representing:

- information technology;
- facilities;
- human resources;
- risk / Business Continuity Management; and
- business areas.

The Committee will meet quarterly, or on a schedule deemed appropriate by the Committee.

BCM Programme Manager

- manage development and implementation of the agency's BCM programme;
- provide input, support and liaison as required to functional areas on the BCM process;
- coordinate regular testing of plans and report results to management;
- coordinate on-going BCM training programme;
- report to management on status of the BCM programme and spend against budget; and
- provide advice to the management team in the event of plan invocation.

BCM Coordinator

- represents the division / department on all BCM matters (single point of contact);
- coordinate completion BCM activities; and
- updates and maintains the division / department's Business Continuity Plans.

Appendix 4 Sample Table of Contents for a BCM Policy

A BCM policy is a concise, formal statement of principles that indicate how the organisation will act in relation to Business Continuity Management. It provides members of the organisation with the approved way of operating and enables decision making on issues pertaining to the BCM process and programme implementation.

Typically, a BCM policy would contain the following key elements:

1. Policy Statement

An overarching statement of what BCM means to the organisation, the importance of BCM to the organisation and the expectations of the organisation on what the BCM programme is to achieve.

2. Scope

The coverage of the policy - for example, does it cover all divisions, subsidiaries or branches? Does it apply only to employees or are contractors subjected to the policy? What about dealings with external service providers, business partners and other stakeholders?

3. Objectives of BCM

Broad aims of the BCM programme for the organisation – for example, what is to be achieved before, during and after an incident, expectations of business continuity timeframes, need for compliance with guidelines and regulatory / statutory requirements, and so on.

4. BCM Planning Parameters

The assumptions, limitations and boundaries of the BCM programme – for example, duration of outage and extent of loss being planned for, availability of people and resources, availability and accessibility of backup data and facilities, and so on.

5. BCM Requirements

What is the agency required to do to fulfil the requirements of its BCM programme – for example, all business areas to conduct a business impact analysis, identify critical processes, document their plans, and test their plans at least twice a year?

6. BCM Roles and Responsibilities

What are the responsibilities of the agency's Board, Executive, managers and employees in relation to business continuity management?

7. Policy Governance

Who in the agency has custody of the BCM policy and how will compliance to the policy be monitored and reported?

8. Effective Date

When does the policy take effect and how often should it be reviewed?

APPENDIX 5 Sample BCM Programme Schedule

	Tasks	Person responsible	Target start date	Target completion date
1	**Programme Management**			
1.1	**Preparation and set-up**			
1.1.1	Appoint BCM programme manager			
1.1.2	Understand organisational structure			
1.1.3	Define BCM process and deliverables			
1.1.4	Develop BCM programme schedule and budget			
1.2	**Risk Management Steering Committee (RMSC)**			
1.2.1	Develop terms of reference for RMSC			
1.2.2	Identify and appoint RMSC members			
1.2.3	Conduct first RMSC meeting			
1.3	**BCM Policy**			
1.3.1	Develop BCM policy document			
1.3.2	Obtain RMSC approval for BCM policy			
1.3.3	Communicate approved BCM policy to employees			
2	**Risk and Business Impact Analysis**			
2.1	**Preparation and set-up**			
2.1.1	Review and understand existing risk analysis			
2.1.2	Customise BIA templates			
2.1.3	Develop list of activities by business areas			
2.2	**Business impact analysis**			
2.2.1	Conduct BIA workshops by business areas			
2.2.2	Consolidate findings and develop business impact profile			
2.2.3	Present business impact profile to RMSC / Executive			
2.3	**Business continuity strategy and requirements**			
2.3.1	Conduct BC strategy and requirements workshops			
2.3.2	Consolidate findings			
2.3.3	Present BC strategy and requirements to RMSC			
3	**Identify Response Options**			
3.1	**Preparation and set-up**			
3.1.1	Form working group			
3.1.2	Review BC strategy and requirements with working group			
3.2	**Response options**			
3.2.1	Identify and evaluate response options for			
	- people			
	- IT systems and networks			
	- premises and facilities			
	- data backup and offsite storage			
3.2.2	Prepare evaluation report			
3.2.3	Present recommendation to RMSC for approval			

4	Develop Response Plan			
4.1	**Preparation and set-up**			
4.1.1	Customise plan formats			
4.2	**Notification and escalation**			
4.2.1	Define notification and escalation process			
4.2.2	Define criteria for plan activation			
4.3	**BCM Plan Overview**			
4.3.1	Draft BCM Plan Overview document			
4.3.2	Submit BCM plan to RMSC for approval			
4.4	**Emergency Response (ER) Plan**			
4.4.1	Review existing ER response plan			
4.4.3	Revise / update ER plan if necessary			
4.5	**Crisis Management (CM) Plan**			
4.5.1	Define CM team structure			
4.5.2	Draft CM plan document			
4.5.3	Submit CM plan to RMSC for approval and sign-off			
4.5.4	Conduct briefing for CM team members			
4.6	**Continuity and Recovery Response (C&RR) Plan**			
4.6.1	Define C&RR team structure			
4.6.2	Conduct C&RR plan development workshops			
4.6.3	Draft C&RR plan documents			
4.6.4	Submit C&RR plans to business heads for sign-off			
4.6.5	Conduct briefing for business continuity teams			
4.7	**Physical implementation**			
4.7.1	Implement IT backup systems and disaster recovery facilities			
4.7.2	Implement business continuity backup site and facilities			
4.7.3	Implement data backup and offsite storage facilities			

5	Train, Exercise and Maintain			
5.1	**Preparation and set-up**			
5.5.1	Identify training, exercise and maintenance requirements			
5.2	**Training**			
5.2.1	Develop training strategy, programme and schedule			
5.2.2	Develop and conduct BCM awareness training for all staff			
5.2.3	Develop and conduct crisis management team training			
5.2.4	Develop and conduct BC training for key appointments			
5.3	**Exercise**			
5.3.1	Develop exercise strategy, programme and schedule			
5.3.2	Develop and conduct crisis management exercise			
5.3.3	Develop and conduct business continuity exercise			
5.3.4	Develop and conduct IT disaster recovery exercise			
5.4	**Maintenance**			
5.4.1	Develop maintenance strategy, programme and schedule			

APPENDIX 6A Sample Risk / Business Impact Reference Table

Level	Rank	Injuries	Financial Loss	Interruption of Service	Reputation & Image	Operational Efficiency	Performance	Stakeholder impact	Regulatory/Statutory
1	**Insignificant**	None	Less than $50,000 or .025% of operational budget	Less than 1 hour	Unsubstantiated, low impact, low profile or no news item.	Little impact	Up to 5% variation in KPI or Objectives	Inconvenience & delays to individuals	No noticeable regulatory/statutory impacts
2	**Minor**	First aid treatment	$50,000 to $250,000 or .15% of operational budget	1 hour to 1 day	Substantiated, low impact, low news profile	Inconvenient delays	5% - 10% variation in KPI or Objectives	Significant impacts on individuals but no noticeable impact on overall service delivery	Minor and temporary non-compliance with regulatory requirements
3	**Moderate**	Medical treatment required	$250,000 to $3 million or 2% of operational budget	1 day to 1 week Loss of building or workspace	Substantiated, public embarrassment, moderate impact, moderate news profile.	Delays in major deliveries	10%-25% variation in KPI or Objectives	Major impacts on significant numbers of individuals, resulting in noticeable impact on overall service delivery	Short-term non-compliance with significant regulatory requirements
4	**Major**	Death or extensive injuries	$3 million – $10 million or 6% of operational budget	1 week to 1 month Loss of building or workspace	Substantiated, public embarrassment, high impact, high news value, Third party actions	Non achievement of major deliverables	20%-50% variation in KPI or Objectives	Major and long term impacts on individuals and overall delivery of services	Significant non-compliance with essential regulatory requirements
5	**Catastrophic**	Multiple deaths or severe permanent disabilities	More than $10 million or more than 6% of operational budget	More than 1 month Loss of building or workspace	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, Third party actions	Non achievement of major key corporate objectives	More than 50% variation in KPI or Objectives	Permanent or debilitating impact on individuals and overall delivery of services	Long-term or indefinite non-compliance with essential regulatory requirements

The purpose of a Risk / Business Impact Reference Table is to provide a common language on how consequences (impacts) are evaluated and measured. The above illustrates various consequence categories that may be used in an agency's risk assessment process. A subset of these categories is used for a Business Impact Analysis (BIA). The categories should reflect the agency's economic, social and environmental responsibilities in relation to business continuity. As an example, the categories that are shaded above are used in the BIA samples illustrated in this Appendix.

Appendix 6B Sample Business Impact Analysis Template

Division / Department:	
Activity:	

This analysis is to be done for each activity in the Division / Department.

Assess the potential business impact on the agency as a whole should this process / activity suffer an outage of varying durations due to a major incident. Assume that all your normal day to day resources (such as computers, data, office facilities, and business records) are not available.

Refer to the Business Impact Reference Table for definitions of the ratings.

	Duration of outage	Impact Rating 1	2	3	4	5
1 Financial Loss						
Could interruption of services lead to financial loss (such as revenues, interest costs, penalties and extra cost of working)?	1 day					
	3 days					
	5 days					
	10 days					
2 Reputation & Image						
Could interruption of services lead to a loss of public confidence, negative publicity and/or damage the image and reputation of the college?	1 day					
	3 days					
	5 days					
	10 days					
3 Stakeholder Impact						
Could interruption of services suspend or restrict expectations of stakeholders?	1 day					
	3 days					
	5 days					
	10 days					
4 Regulatory/Statutory						
Could interruption of services breach statutes/regulations?	1 day					
	3 days					
	5 days					
	10 days					
OVERALL RATING						
Based on the above impacts, provide an overall impact rating for this process / activity	1 day					
	3 days					
	5 days					
	10 days					

Comments -	Maximum Acceptable Outage (MAO)

Person/s interviewed : Date:
Facilitators:

Appendix 6C Sample List of Business Activities

Agency name: Sample Agency

Division	Department	Activity
Business Services	Licensing Centre	Provide specialist advice
		Process applications and renewals
		Compliance monitoring
	Business Advisory	Provide advocacy services
		Provide referral services - overseas markets
		Provide referred services - domestic markets
	Event Management	Conduct market research
		Development and organise events
		Conduct public workshops
Policy and Planning	Policy Planning	Planning, forecasting and data analysis
		Policy development and management
	Compliance	Monitor programme compliance
Corporate Services	Human Resources	Provide recruitment services
		Oversee OSH compliance
		Administer staff entitlements and payroll
		Manage training and development
	Information Technology	Run data centre operations
		Develop and maintain business applications systems
		Provide users helpdesk support
	Finance & Administration	Manage budgeting and reporting processes
		Perform financial accounting functions
		Manage building services and maintenance
		Manage goods and services procurement
Office of the CEO	-	Manage corporate communications and public relations
		Manage State and Commonwealth relationships

Appendix 6D Sample Business Impact Analysis

Division / Department:	Business Services / Licensing Centre
Activity:	Provide Specialist Advice

This analysis is to be done for each activity in the Division / Department.

Assess the potential business impact on the Agency as a whole should this process / activity suffer an outage of varying durations due to a major incident. Assume that all your normal day to day resources (such as computers, data, office facilities, and business records) are not available.

Refer to the Business Impact Reference Table for definitions of the ratings.

	Duration of outage	Impact Rating 1	2	3	4	5
1 Financial Loss						
Could interruption of services lead to financial loss (such as revenues, interest costs, penalties and extra cost of working)?	1 day	✓				
	3 days	✓				
	5 days	✓				
	10 days	✓				
2 Reputation & Image						
Could interruption of services lead to a loss of public confidence, negative publicity and/or damage the image and reputation of the college?	1 day	✓				
	3 days	✓				
	5 days		✓			
	10 days			✓		
3 Stakeholder Impact						
Could interruption of services suspend or restrict expectations of stakeholders?	1 day	✓				
	3 days	✓				
	5 days		✓			
	10 days			✓		
4 Regulatory/Statutory						
Could interruption of services breach statutes/regulations?	1 day	✓				
	3 days	✓				
	5 days	✓				
	10 days	✓				
OVERALL RATING						
Based on the above impacts, provide an overall impact rating for this process / activity	1 day	✓				
	3 days	✓				
	5 days		✓			
	10 days			✓		

Comments - This department provides ad hoc advice to businesses on specialised areas related to licensing such as legislation and regulations. Volume of enquiries tend to be low on most days. If services are not available, the clients may obtain the information from other agencies	Maximum Acceptable Outage (MAO) **May be deferred > 10 days**

Person/s interviewed : Date:
Facilitators:

Appendix 6E Sample Business Impact Analysis

Division / Department:	Business Services / Licensing Centre
Activity:	Process Applications and Renewals

This analysis is to be done for each activity in the Division / Department.

Assess the potential business impact on the agency as a whole should this process / activity suffer an outage of varying durations due to a major incident. Assume that all your normal day to day resources (such as computers, data, office facilities, and business records) are not available.

Refer to the Business Impact Reference Table for definitions of the ratings.

	Duration of outage	Impact Rating				
		1	2	3	4	5
1 Financial Loss						
Could interruption of services lead to financial loss (such as revenues, interest costs, penalties and extra cost of working)?	1 day	✓				
	3 days	✓				
	5 days	✓				
	10 days	✓				
2 Reputation & Image						
Could interruption of services lead to a loss of public confidence, negative publicity and/or damage the image and reputation of the college?	1 day	✓				
	3 days		✓			
	5 days			✓		
	10 days				✓	
3 Stakeholder Impact						
Could interruption of services suspend or restrict expectations of stakeholders?	1 day	✓				
	3 days			✓		
	5 days				✓	
	10 days				✓	
4 Regulatory/Statutory						
Could interruption of services breach statutes/regulations?	1 day	✓				
	3 days		✓			
	5 days			✓		
	10 days				✓	
OVERALL RATING						
Based on the above impacts, provide an overall impact rating for this process / activity	1 day	✓				
	3 days			✓		
	5 days				✓	
	10 days				✓	

Comments - The Dept will not be able to collect licensing fees if the outage is prolonged but this will not result in any direct financial loss as collections are merely deferred. Key impact would be on clients as non-renewal of license would force them to close to avoid violating regulations. As a result, the public repercussions on the Dept could be serious. Workarounds need to be put in place for the processing of renewals.	Maximum Acceptable Outage (MAO) **5 days**

Person/s interviewed : Date:

Facilitators:

Appendix 6F Sample Consolidated Business Impact Profile

Agency name: Sample Agency

Division	Department	Activity	Maximum Acceptable Outage				
			1 day	3 days	5 days	10 days	Deferred
Business Services	Licensing Centre	Provide specialist advice					✓
		Process applications and renewals			✓		
		Compliance monitoring					✓
	Business Advisory	Provide advocacy services			✓		
		Provide referral services - overseas markets				✓	
		Provide referred services - domestic markets				✓	
	Event Management	Conduct market research					✓
		Development and organise events					✓
		Conduct public workshops					
Policy and Planning	Policy Planning	Planning, forecasting and data analysis					✓
		Policy development and management					✓
	Compliance	Monitor programme compliance					✓
Corporate Services	Human Resources	Provide recruitment services					✓
		Oversee OSH compliance					✓
		Administer staff entitlements and payroll					✓
		Manage training and development					✓
	Information Technology	Run data centre operations			✓		
		Develop and maintain business applications systems					✓
		Provide users helpdesk support			✓		
	Finance & Administration	Manage budgeting and reporting processes					✓
		Perform financial accounting functions				✓	
		Manage building services and maintenance					✓
		Manage goods and services procurement					✓
Office of the CEO	-	Manage corporate communications and public relations			✓		
		Manage State and Commonwealth relationships			✓		

Appendix 6G Sample Business Continuity Requirements

Agency:	Sample Agency
Division / Department:	Business Services / Licensing Centre

Prioritisation of activities (based on the MAOs defined in business impact analysis)

		Prioritisation (MAO)				
Ref	**Activity**	**1 day**	**3 days**	**5 days**	**10 days**	**Deferred**
LC-1	Provide specialist advice					✓
LC-2	Process applications and renewals			✓		
LC-3	Compliance monitoring					✓

Business continuity strategy overview

Outline the strategy for continuing the priority activities listed above over the various timeframes, taking into consideration any interdependencies with other divisions or external parties, volume of transactions that could be handled, etc)

1 day	Redirect all queries to agency's web site and 1800 service; Inform public of office closure through signage and media announcements; Inform other relevant agencies; Establish status of applications being processed
3 days	
5 days	Defer all new applications and only process renewals at alternate site;
10 days	Resume processing of new applications at alternate site

Resource requirements

	Cumulative quantities required			
	1 day	**3 days**	**5 days**	**10 days**
Minimum staffing levels:				
Managers	1	1	1	2
Officers and support staff	1	1	5	7
Office equipment:				
Personal computer	-	1	6	9
Laser printer - black and white	-	1	1	1
Laser printer - colour	-	-	-	-
Standard phone	-	2	6	9
Fax	-	1	1	1
Photocopier	-	-	1	1
Others:				

System / application requirements

	Tick (✓) those required within....			
Name of system / application	**1 day**	**3 days**	**5 days**	**10 days**
Microsoft Office		✓	✓	✓
Internet access		✓	✓	✓
E-mail		✓	✓	✓
Oracle Finance System				
COGNOS				✓
TRIM			✓	✓
Client Management System				✓

Vital records / reports / forms / documentation requirements (on server)

		Tick (✓) those required within....			
Name of vital record / report / form / documentation	**Location (server / drive name)**	**1 day**	**3 days**	**5 days**	**10 days**
Corporate shared data	Edna\Data\G:\		✓	✓	✓
Licensing database	Kdna\Lic\POS\			✓	✓

Vital records / reports / forms / documentation requirements (paper-based)

		Tick (✓) those required within....			
Name of vital record / report / form / documentation	**Frequency of backups and storage location**	**1 day**	**3 days**	**5 days**	**10 days**
Licensing Form 814	8th flr store room			✓	✓
Licensing Form 815	8th flr store room			✓	✓
Client files	Grd flr cabinets				✓

Interdependencies with internal parties

		Tick (✓) those required within....			
Name of external party	**Interactions required**	**1 day**	**3 days**	**5 days**	**10 days**
Finance & Admin	Process payments			✓	✓

Interdependencies with external parties

		Tick (✓) those required within....			
Name of external party	**Interactions required**	**1 day**	**3 days**	**5 days**	**10 days**
Australian Taxation Office	Request for info			✓	✓

Appendix 7A Sample Terms of Reference: Crisis Management Team

Purpose of the Crisis Management Team

The Crisis Management Team (CMT) consists of a small group of executives who have the resources, ability and authority to do whatever is necessary to resolve a crisis. The team will take operational ownership of the crisis response when:

- a crisis has occurred; or
- when a possible or probable crisis situation will exist if a threatening event materialises.

The CMT is the highest level decision making authority at times of crisis. It has unrestricted authority to respond in the best interest of all stakeholders and its crisis response decisions will supersede the existence or normal interpretation of all or any policy or standard operating procedures.

Roles and Responsibilities

The CMT is made up of the following roles:

ROLE	RESPONSIBILITIES
Crisis Manager / Team Leader	• Provides overall leadership • Liaises with Board and CEO • Allocates resources, sets priorities and resolves conflicts • Briefs the company spokesperson
Command Centre Coordinator	• Keeps command centre functioning including supporting technologies and resources • Maintains status board of crisis and call register
Corporate Communications	• Single source of information to internal and external stakeholders and media • Media management
Human Resources	• Provide employee assistance such as medical assistance, counselling, insurance claims, payroll duties etc • Emergency evacuation/repatriation • Liaise with victims' families • Provide recruitment support
Corporate Security	• Ensures staff safety • Liaise with Emergency Services • Monitors emergency response • Security of assets and staff • Communicate with external parties on security intelligence

ROLE	RESPONSIBILITIES
Administration and Logistics Support	• Facilitates and supports recovery efforts, may consist of food services, transport arrangements, mail duties, insurance, legal, finance requirements etc
Premises and Facilities	• Coordinates damage assessment, salvage and repair operations and reconstruction • Supports insurance claim process • Plans for relocation to primary site
Business Recovery Coordinator	• Coordinates execution of business recovery plans • Provides status updates to crisis management team
IT Recovery Coordinator	• Coordinates execution of IT recovery plans • Resolve systems, networks and applications issues • Provides status updates to crisis management team

Crisis Management Plan

A Crisis Management Plan sets out the principles to be followed should any incident cause, or threaten to cause, serious business impact to the organisation.

The plan provides a process that facilitates organised decision-making in the event of a major incident that might otherwise be quite chaotic and to:

- minimise injury or loss of life and protect the safety of staff and visitors;
- provide a flexible response process for a variety of emergencies;
- focus decision making on critical issues in a potentially stressful environment; and
- minimise the negative consequences of any incidents on the Insurance Commission, staff and visitors.

The plan suggests actions to take and is only guidelines to serve in managing a major incident. Real life decisions for reacting to a major incident must be guided ultimately by the sound judgement and discretion of involved managers and staff.

Appendix 7B Sample Terms of Reference: Business Continuity Teams

Purpose of the Business Continuity Teams

The Business Continuity Teams are responsible for ensuring that critical business activities are resumed according to the re-established prioritisation and within the required timeframes.

The Teams are mobilised upon activation of the agency's BCM plan by the Crisis Management Team. The number of teams required depends on the nature and size of the agency but typically there will be at least one team per department / functional area.

Roles and responsibilities

A Business Continuity Team is made up of the following roles

ROLE	RESPONSIBILITIES
Team Leader	▪ Provides overall leadership to the team ▪ Ensures that critical activities are restored within the required timeframes ▪ Keeps the Crisis Management Team appraised of business continuity progress
Alternate Team Leader	▪ Acts as a backup to the Team Leader
BCM Coordinator	▪ Assist the Team Leader as required ▪ Coordinate communications within the team and liaise with other areas of the agency ▪ Maintain a status board on the team's business continuity progress
Team Members	▪ Carry out business continuity tasks in accordance with the team's Business Continuity and Recovery Plan
Stand-by Team Members	▪ Be on stand-by at home ▪ Provide any assistance with business continuity tasks when called upon ▪ Support long term recovery task when required

Appendix 8A Sample Table of Contents: BCM Plan Overview

1. Version control information
2. Distribution list
3. Purpose of the BCM Plan
4. Objectives of the BCM Plan
5. BCM Policy
6. BCM Process Overview
7. Critical Business Activities
    a. Maximum Acceptable Outage
    b. Interdependencies
8. Business Continuity Strategies and Requirements
    a. Broad Strategies
    b. Resource Requirements
    c. Systems and Applications Requirements
9. Response Options
    a. Planning Parameters
    b. Business Continuity Site
10. Response Plan
    a. Guiding Principles
    b. Crisis Management Organisation
        i. Crisis Management Team
        ii. On Scene Response Team
        iii. Crisis Support Teams
        iv. Business Continuity Teams
        v. IT Disaster Recovery Team
    c. Notification and Escalation Process
    d. Command Centre
11. Training, Exercise and Maintenance
    a. Training Requirements and Protocols
    b. Exercise Requirements and Protocols
    c. Maintenance Requirements and Protocols

Appendix 8B Sample Table of Contents: Emergency Response Plan

Appendix 8C Sample Table of Contents: Crisis Management Plan

1. Purpose

    1.1. Outlines the purpose of the plan and circumstances under which the plan is to be used

2. Definition of Crisis Events

    2.1. Defines what constitutes a crisis event that would lead to the activation of the Crisis Management Plan

3. Crisis Management Team Structure

    3.1. Outlines the purpose and membership of the Crisis Management Team
    3.2. Describes the roles and responsibilities of the team members

4. Notification and Escalation Process

    4.1. Outlines the process by which an incident is reported, assessed, and escalated through various levels of management, leading to the activation of the Crisis Management Team

5. Command Centre

    5.1. Describes the purpose of the command centre, its location and resources that should be made available to support the Crisis Management Team

6. Communications During a Crisis

    6.1. Describes the communications protocols and tools to be used, how events are to be tracked and recorded and how status updates are to be communicated in a crisis situation

7. Contact lists

    7.1. Contact lists of the Crisis Management Team members, senior management, key staff, service providers, emergency services and other stakeholders who may need to be informed and / or are needed to provided assistance during a crisis situation

8. Actions check lists

    8.1. Checklists of issues and actions that the Crisis Management Team need to consider for crisis management response and business continuity. These serve as reminders to ensure that no critical issues or actions are forgotten in the confusion and chaos that may result in a crisis situation.

Appendix 8D Sample Continuity and Recovery Response Team Action Plan

CONTINUITY AND RECOVERY RESPONSE

TEAM ACTION PLAN

For

{division name}

Version x.x dd mm yyyy

Version Control

Version	Release date	History
1.0	dd/mm/yyyy	

Distribution

This plan has been distributed to the following:

Name	Position / function

Holders of this plan are to ensure that they keep a copy of this plan in the office as well as a copy at home.

Table of Contents

Version Control

Distribution

Table of Contents

1.0 Purpose

The Business Continuity Team Action Plan outlines the actions to be taken and resources to be used to facilitate the continuity of critical business activities in the event of prolonged business interruption due to major incident impacting the agency.

This plan is not a complete, step-by-step, how-to-do-it manual since each crisis situation is unique, with varying levels of threats and business impact.

The plan suggests actions to take and is only guidelines to serve in managing a major incident. Real life decisions for reacting to a major incident must be guided ultimately by the sound judgement and discretion of involved managers and staff.

Procedures for dealing with day-to-day problems are not dealt with in this plan. Such problems should be taken up under the agency's standard operating procedures.

2.0 Team Charter

The role of this team is to ensure the continuity of critical activities of ***{Division name}*** within the stipulated timeframes in the event of a major incident that renders the premises of the ***{Agency name}*** inaccessible or unusable.

The key responsibilities of this team are:

-
-
-

3.0 Team Composition

Team Leader	
Alternate Team Leader	
BCM Coordinator	

Team Members	

Stand-by Team Members	

4.0 Critical Business Activities and Strategy

The critical business activities and their corresponding Maximum Acceptable Outage (MAO) of this Division are as follows:

		Maximum Acceptable Outage			
Division	Activity	1 day	3 days	5 days	10 days

Other activities that are not listed in the table will be deferred in the event of BCP invocation. Although these deferred activities may be important for the day to day operations of the agency, they are not deemed to be critical under business continuity situations.

Deferred activities will be restored during the long term recovery phase – the level of effort, allocation of resources and actions needed would be dependent on the nature of the incident.

The broad strategies for the continuation of critical business activities are as follows:

	1 day	3 days	5 days	10 days
Strategy				

5.0 Assessment and Notification

5.1 Incidents during office hours

Initial Alert

Ref	Action	Done
1	If you become aware of a security event, contact the Security or your OSH representative	
2	Inform your manager of the incident	

Evacuation

Ref	Action	Done
3	When alarm is sounded, evacuate to the muster point as directed. Follow the instructions of your Floor Warden	
4	When you are at the muster point, ensure that you record your attendance with your Floor Warden	

Initial Assessment

Ref	Action	Done
5	The Crisis Management Team will assess the situation and decide if the Business Continuity Plan is to be invoked	
6	If the Business Continuity Plan is not invoked, return to the building when instructed by your Floor Warden	

Plan Invocation

Ref	Action	Done
7	If the Business Continuity Plan is invoked: a. Instruct relevant team members to proceed to the Business Continuity site b. Instruct team members who are not required immediately to support business continuity to return home to wait for further instructions	

5.2 Incidents outside office hours

Initial Alert

Ref	Action	Done
1	When you receive the notification, confirm with the caller: a. Nature of the problem and circumstances leading to the Business Continuity Plan invocation b. Phone number where the caller can be reached c. That you will do the necessary notification to your Team Leader, if necessary	

Initial Assessment

Ref	Action	Done
2	If necessary, notify your Team Leader: When you call, provide the following information: a. Nature of the problem and circumstances leading to the Business Continuity Plan invocation b. Phone number where you can be reached Discuss with your Team Leader the key actions to be taken and who in the team should be activated	

Plan Invocation

Ref	Action	Done
3	Notify your Team members. When you call, tell them that the Business Continuity Plan has been invoked Ask them to proceed to the Business Continuity site immediately and to bring along a copy of their Business Continuity Team Action Plan, mobile phone, and access card Remind them not to speak with any external parties, including the media about the invocation	

6.0 Phase 2 Plan Activation

6.1 Upon Arrival at Business Continuity Site

Ref	Action	Done
1	Verify that all required equipment are available and operational Verify that all required application systems are operational Notify IT User Support or Facilities if you encounter any problems with the IT / office infrastructure	
2	Re-establish positions of all work-in-progress and lost transactions, if any	
3	Retrieve and check supplies and vital records from off-site storage. If necessary, place orders for additional supplies	

6.2 Business Resumption

Within 1 day

Ref	Action	Done
1		
2		
3		
4		
5		

Within 3 days

Ref	Action	Done
1		
2		
3		
4		
5		

Within 5 days

Ref	Action	Done
1		
2		
3		
4		
5		

Within 10 days

Ref	Action	Done
1		
2		
3		
4		
5		

7.0 Phase 3 Return to Normalcy

7.1 Damage Assessment

	Action	Done
1	The Crisis Management Team will decide when would be an appropriate time to conduct a detailed damage assessment	
2	Assign 2 staff to participate on the Damage Assessment Team	
3	Carry out damage assessment under the direction of the Damage Assessment Team Leader	

7.2 Salvage and Restoration

	Action	Done
1	Compile list of items from the department that can be salvaged and those that have to be replaced	
2	Work with IT and Facilities to identify requirements for new office	

7.3 Relocation

	Action	Done
1	Following the decision of the Crisis Management Team to relocate determine the move requirements	
2	Develop plan to relocate processing back to the primary office, ensuring to maintain data integrity through the process	

Appendix 1 Contact Lists

Team Members (Primary)

Function	Name	Work Tel #	Mobile #	Home Tel #
Team Leader				

Team Members (Designated Alternates)

Function	Name	Work Tel #	Mobile #	Home Tel #

Other internal contacts

Function	Name	Work Tel #	Mobile #	Home Tel #

External contacts (Service providers, government agencies, etc)

Organisation	Contact Person	Number	Comments

Appendix 2 Resource Requirements

	Cumulative quantities required within …			
	1 day	3 days	5 days	10 days
Minimum staffing levels:				
Managers				
Officers				
Office equipment:				
Desktop computer (stand alone)				
Desktop computer (networked)				
Laptop computer				
Modem				
Mono-laser printer				
Colour Printer				
Phone				
Fax				
Photocopier				
Typewriter				
Calculator				
Others:				

Appendix 3 System / Application Requirements

	Tick (□) those required within …			
Name of system / application	1 day	3 days	5 days	10 days

Appendix 4 Vital Records Requirements

Vital records / reports / forms / documentation requirements (on server)

		Tick (□) those required within …			
Name of vital record / report / form / documentation	**Location (server / drive name)**	**1 day**	**3 days**	**5 days**	**10 days**

Vital records / reports / forms / documentation requirements (paper-based)

		Tick (□) those required within …			
Name of vital record / report / form / documentation	**Frequency of backups and storage location**	**1 day**	**3 days**	**5 days**	**10 days**

Appendix 9 Sample BCM Programme Review Checklist

	Yes	No	Remarks
Plan Scope			
1. Have specific objectives of the plan been defined? Do the objectives appear reasonable?			
2. Does the scope of the plan appear reasonable to the present operations of the agency and that there is valid justification for any areas that have been excluded?			
3. Do the assumptions made in the plan appear reasonable and take into consideration the current risk factors faced by the agency?			
Business impact assessment			
1. Have all business units / processes been assessed to determine their criticality to the agency?			
2. Do the criteria used to determine criticality appear reasonable?			
3. Have recovery timeframes (or maximum tolerable outage) for each critical activity been identified?			
4. Have the minimum business continuity resource requirements for critical business activities been identified?			
Response Options			
1. Has a detailed analysis of various alternative treatment (recovery) options, including internal options, which can support the agency's business continuity requirements been carried out?			
2. Were specific selection criteria defined and used in the evaluation of treatment options, and do they appear reasonable?			
3. Does the selected treatment option for each of the critical business activities appear reasonable and capable of supporting the current operations?			
4. Do the treatment options provide for a smooth integration of the components applicable to different departments in different locations within the agency?			

	Yes	No	Remarks
5. Where third party services are used, does the contract appear reasonable?			
Plan Content			
Disaster notification and escalation 1. Is the disaster notification and plan activation procedure clearly documented?			
2. Are there management procedures for monitoring of a situation and incident escalation?			
3. Do the procedures provide for a decision tree approach to help guide the management team under situation of intense pressure?			
4. Do the incident escalation procedures involve appropriate civil authorities and other external agencies?			
5. Are there procedures for handling the media and communications with internal and other external parties?			
Business continuity procedures 6. Do the numbers and composition of recovery teams appear reasonable and consistent with the BCP needs of the agency?			
7. Do the procedures for transporting staff and materials appear reasonable?			
8. Are manual continuity procedures written in a format of sufficient details that could easily be followed?			
9. Do the continuity procedures provide for on-going checkpoints on the success of the operations and fall back positions?			
10. Do the continuity procedures provide for controls over the completeness and accuracy of the process?			
Recovery (return to normal) procedures 11. Is there a process for conducting damage assessment post-disaster?			
12. Do the salvage and refurbishment procedures appear reasonable?			

	Yes	No	Remarks
13. Do the procedures address the 'return to normal' operations in a controlled manner?			
14. Do the procedures for the 'return to normal' operations appear to be reasonable?			
Training			
1. Is there regular and pre-defined training that is to be performed in accordance with a structured programme?			
2. Does the training programme appear reasonable and appropriate?			
3. Is there a process to ensure that all staff receive regular refresher training?			
4. Has BCM awareness been incorporated into the staff induction training?			
Exercising / Testing			
1. Is there a regular and pre-defined schedule of exercises?			
2. Does the exercise schedule appear reasonable and appropriate?			
3. Is there a pre-defined methodology for exercising various components of the plan?			
4. Are results of tests being documented in accordance with the defined methodology?			
5. Are post-mortems being held after each test?			
Maintenance			
1. Has responsibility for plan maintenance or administration been assigned to specific individuals?			
2. Is there a regular and pre-defined schedule for plan maintenance?			
3. Does the plan maintenance schedule appear reasonable?			
4. Does the plan maintenance process outline conditions which should automatically trigger plan updates?			

	Yes	No	Remarks
5. Does the plan maintenance process provide for control over the completeness and accuracy of changes, as well as approval for making documentation changes?			