Business Continuity Plan Guide

Prepared for

Carol MacDonald, PhD

February 2014

Contents

What is a business continuity plan?

Business continuity planning is one element of a Business Continuity process that helps an organisation to anticipate, prepare for, respond to and recover from major disruptions. Business Continuity Management provides an organisation with a process for identifying and managing risks that could disrupt normal service and prevent it from achieving its objectives.

Developing a Business Continuity Plan will assist you to manage the risks to ensure that, at all times, your business can continue operating to at least a pre-determined minimum level. This will enable you to continue service delivery during and beyond crisis. It is about anticipating the hazards or threats that could affect your organisation and planning for them to ensure that it can continue to function in the event of a disruption, whatever the cause and whatever part of the business is affected.

The Business Continuity Plan documents the roles and responsibilities, procedures, resources, services, activities and processes required to ensure the continuity and recovery of critical business functions following disruption.

About this guide

There is no 'one-size-fits-all' approach to developing a Business Continuity Plan. The purpose of this guide is to assist you to design and implement a Business Continuity planning process that is appropriate to your needs. These needs are shaped by legal, regulatory, organisational and sector requirements, the functions and services, other processes, the size and structure of the organisation, and the requirements of its stakeholders.

Ideally the Business Continuity Plan is developed as part of a comprehensive Business Continuity Management process. Recognising that this will not be possible for all NASCs, this guide incorporates key elements of the Business Continuity Management process into the accompanying template and the Business Continuity Planning process that it reflects. The guide outlines simplified Business Continuity Planning steps that can help the organisation plan for and recover from a major disruption. These steps cover three phases:

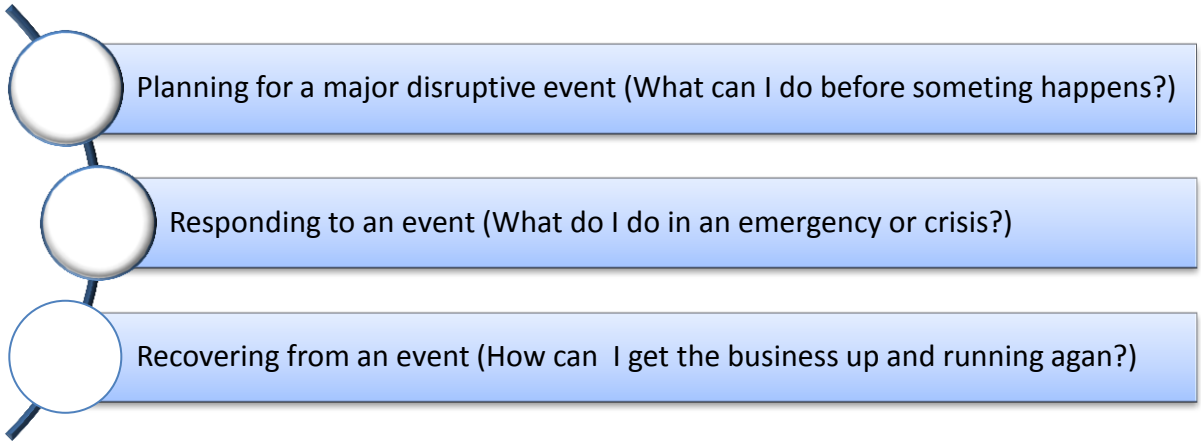

Figure 1: Phases in Business Continuity Management

The guide is structured to reflect these phases and provides tables, checklists and examples for each step in the planning process. You should customise the template to suit the needs of your organisation so that it is relevant to its objectives, size, complexity and location. The *blue sample text* is there to provide examples or guide you and can be deleted after you have completed the template.

Template:
You will find these text boxes throughout the guide to assist you to complete the template.

Basic emergency procedures

Ensure that basic emergency procedures are in place before starting the Business Continuity Plan. The emergency procedures cover the actions required during the immediate response to a major incident or emergency. The Business Continuity Plan deals with what you need to continue and recover critical business functions following the disruption caused by the emergency. Emergency procedures should be brief, concise documents (flip charts are useful) which show clear process, roles and responsibilities in the event of emergencies such as fire, earthquake, flood or water damage, violent behaviour etc. All staff should know where to locate the "guidelines and procedures document" and be aware of what is expected of them.

Planning for a disruptive event

Completed Business Continuity Plan Checklist

The checklist at the front of the template is provided as a summary of the items that can be included in your business plan and the key elements of the Business Continuity planning process. Complete the checklist as you progress through the planning process. Customise it to meet the needs of your business and to reflect any modifications you make to the template.

Template:
Customise and complete ***Table 1: Checklist of Items to include in the Business Continuity Plan***.

Version Control

When updating the plan(s) an effective system of version control should be adopted and maintained. Table 2 in the template is provided as an example for organisations without an existing Document Version Control procedure.

Template:
Complete ***Table 2: Version Control*** each time the Business Continuity plan is revised.

Related documents

Organisations may have a number of interrelated documents covering emergency and recovery management and other policy or management issues that may impact on business continuity planning and management. These may include organisational policies, plans, and procedures, the National Health Emergency Management Plan and the local DHB Health Emergency Plan. Both of these plans are relevant to all health services and providers.

Template:
Complete ***Table 3: Related Documents*** listing all documents that have a significant bearing on the Business Continuity Plan.

Understanding your organisation

It is important to have a clear and agreed understanding of your organisation's business objectives, and the critical business functions and processes which ensure those objectives are met. This is a crucial element which enables you to determine appropriate business continuity options.

Business Impact Analysis

Business Impact Analysis involves identifying and documenting the:

- organisation's operational objectives and deliverables
- organisation's key services or products and critical functions required to deliver these
- dependencies (both internal and external) relied on to maintain the critical functions
- impact that a disruption of the critical functions would have on the organisation
- how long your business could survive without performing this function
- priorities and timeframes for resuming the critical functions following disruption
- key resources required for recovery and resumption of business.

The approach used to complete the Business Impact Analysis will depend on the size, type and complexity of the organisation. In a large organisation it is important to involve a range of individuals with a detailed knowledge of the specific functions and activities across the organisation. In smaller organisations an individual or small team may have sufficient knowledge of the organisation to complete this task.

The Business Impact Analysis can be completed as a six step process as depicted in Figure 2.

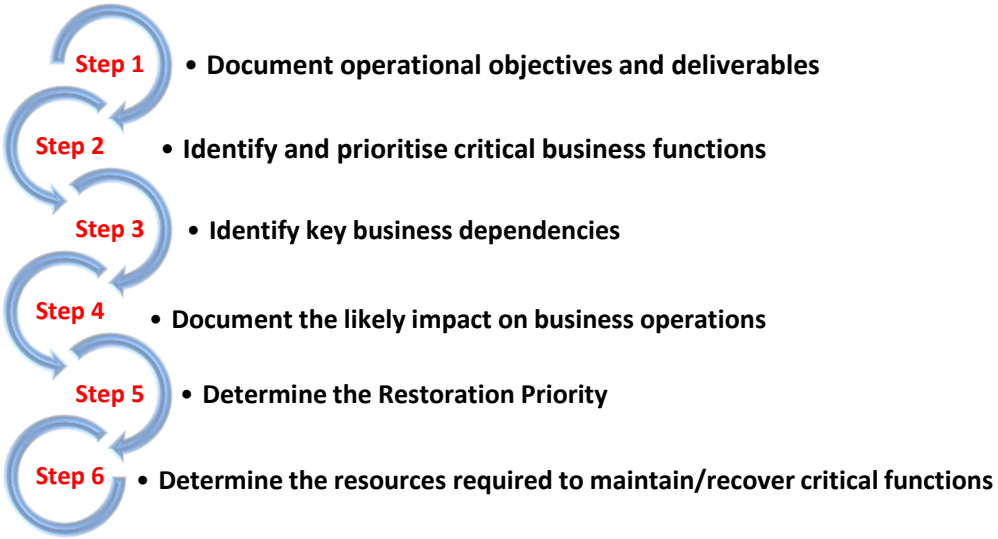

Figure 1: Six steps for a Business Impact Analysis

Step 1: Document the organisation's operational objectives and deliverables.

List the key business objectives and deliverables of your organisation. You could also briefly describe the business, what it does, how it is structured etc. A good starting point is to examine the high-level planning and contractual documents such as service specifications and operational plans.

Template:
Complete ***Table 4: Business objectives and deliverables***

Step 2: Identify and prioritise the organisation's critical business functions.

Identify your critical business functions. These are the functions (and processes) which, if disrupted, will have the greatest impact on the organisation's ability to deliver outputs and achieve objectives.

Template:
Complete column 1 of ***Table 5: Critical Functions Priority List***

Now rank the critical functions in order of their importance to the organisation. Think about how each function contributes to:

- your ability to meet statutory obligations for service delivery
- other business functions (inter-dependency)
- your ability to meet key stakeholder expectations
- cash flows essential to business operations
- maintaining your organisation's reputation.

Template:
Complete column 2 of ***Table 5: Critical Functions Priority List***

You could also briefly describe each critical function, including why it is important to business operations.

Step 3: Identify business dependencies

Who is it that you rely on to provide information/resources or to complete a process or an activity to ensure the successful operation of your business?

For example, you may be dependent on receiving information from another organisation as an input to one of your critical functions or processes. You should also consider internal dependencies between units or departments within your organisation.

Template:
Complete column 3 of ***Table 5: Critical Functions Priority List***

Conversely, external agencies and organisations may be dependent on the output of your organisation to deliver a critical business process of their own.

Step 4: Document the likely impact on business operations

For each critical function identified in Step 1, determine what impact the loss of the function is likely to be for specified time frames (e.g. first 24 hours, 24-48 hours, 1 week or an extended period of disruption).

Consider what the impact would be on your organisation's ability to meet its aims and objectives, and the impact on your stakeholders. How necessary will the function be in an emergency?

Template:
Complete ***Table 6: Impact on business operations*** for each critical function.

Step 5: Determine the Restoration Priority

This step is about determining the priority for resuming critical functions. It involves estimating how long the business can continue to operate without each critical function before it will have a detrimental effect.

Template:
Enter the Restoration Priority in ***Table 6: Impact on business operations***

Table 1: Restoration Priority Scale

Function needs to resume within:	Priority
24 hours	Vital
2-3 days	High
1 week	Moderate
1 month	Low
More than 1 month	Very Low

Determine the Restoration Priority by setting a target time frame for when each function needs to resume.

Use the scale in Table 1 (you may want to customise the time frames).

Step 6: Determine the resources required to maintain/recover critical functions

Document the resources required to maintain or recover the critical functions at an acceptable level? These may include: people, premises, technology, information, supplies and partners. Refer to Table 2 below for a list of questions to consider when determining the minimum resource requirements. Remember that the resources required to resume a function after a disruption will not necessarily be the same as during normal operations as additional resources may be needed to clear backlogs.

Template:
Complete ***Table 7: Minimum Resource Requirements***

Table 2: Considerations when determining resources needed (not an exhaustive list)

PEOPLE	**Key Staff:** What staff do you require to carry out your key functions?	**Skills / Expertise / Training:** What skills/level of expertise is required to undertake these functions?	**Minimum Staffing Levels:** What is the minimum staffing level with which you could provide some sort of service?
PREMISES	**Buildings:** What locations do your department's key functions operate from? (Primary site, alternative premises)	**Facilities:** What facilities are essential to carry out your key functions?	**Equipment / Resources:** What equipment / resources are required to carry out your key functions?
PROCESSES	**IT:** What IT is essential to carry out your key functions?	**Documentation:** What documentation / records are essential to carry out your key functions, and how are these stored?	**Systems & Communications** What systems and means of communication are required to carry out your key functions?
PROVIDERS	**Reciprocal Arrangements:** Do you have any reciprocal agreements with other organisations?	**Contractors / External Providers:** Do you tender key services out to another organisation? If so - to whom and for what?	**Suppliers:** Who are your priority suppliers and whom do you depend on to undertake your key functions?
PROFILE	**Reputation:** Who are your key stakeholders?	**Legal Considerations:** What are your legal, statutory and regulatory requirements?	**Vulnerable Groups:** Which vulnerable groups might be affected if your organisation fails to carry out key functions?

Hazard/Risk Assessment

Risk assessment considers the likelihood and impact of a variety of hazards/threats that could disrupt your critical functions and supporting resources.

Put simply you need to ask:

- What could happen?
- How bad could it be?
- How likely is it?
- What would it mean for the business?

Understanding risks allows you to make informed decisions about how to manage risk by reducing it or preparing for it.

All major hazards that may occur should be considered, and then, having identified the likelihood of each occurring and the likely consequences, risks should be prioritised and ranked. A four step process for completing a risk assessment follows.

Step 1: Identify and document the risk to the organisation

The National Hazardscape Report (2007) identifies 17 types of hazards which all have the potential to cause emergencies. Information from this report was used to create the Table 3 below which presents a range of risks and consequences for the health sector. Use the list of hazards in the table to identify which have the most relevance for your business.

Template:
Complete column 1 ***Table 8: Hazards and risks***

Step 2: Determine the impact each hazard may have on the business.

The risk analysis in Table 3 identifies a range of risks/consequences for each major hazard or threat. This table provides a general starting point for your risk assessment.

Ask, is the hazard likely to:

- Cause physical damage to buildings?
- Cause death or injury?
- Result in the loss of one or more utilities or services?
- Have an impact on staff or their families?

There are no right or wrong answers and risks/consequences are likely to be repeated for different hazards. Plan for worst-case scenarios. If the plan covers how to get back in business if a flood destroys the building, it will also work if only one floor is flooded.

Template:
Complete column 2 ***Table 8: Hazards and risks***

Table 3: Hazard and risks/consequences for the Health Sector

Hazard	Risks /consequences
Animal/ & plant pests & disease	• Isolation of services / staff / patients / communities
Coastal hazards (e.g. Storm surge & erosion)	• Inundation of health services, staff homes, etc., in low-lying areas • Access to premises/site compromised or denied
Drought	• Water supplies reduced
Earthquakes	• Damage to facilities and/or critical infrastructure • Impact on staff and families (physical, social, homes, transport, etc.)
Extreme weather incidents	• Critical infrastructure compromised
Floods	• Damage to facilities and/or critical infrastructure (in low-lying areas) • Loss/contamination of essential drugs and supplies • Isolation of services / staff / patients / communities • Loss of staff/health workers • Water supplies contaminated and/or reduced
Food safety/ contamination	• Health service catering contamination • Loss of staff/health workers
Hazardous substance incidents	• Health impacts/injuries to responders and/or health workers
Human disease pandemic	• Impact on staff and families (physical, social, homes, transport, etc) • Critical services compromised
Infrastructure failure	• Critical services compromised • Communication impacted
Landslides	• Damage to facilities and/or critical infrastructure (in slip zone)
Major transport accidents	• Damage to or contamination of facilities and/or critical infrastructure • Access to site compromised • Patient transport compromised
Severe winds	• Damage to facilities and/or critical infrastructure
Snow	• Damage to facilities and/or critical infrastructure (due to snow-loading) • Isolation of services /staff/patients/communities
Terrorism	• Damage to or contamination of facilities and/or critical infrastructure • Critical services compromised • Damage to or contamination of facilities and/or critical infrastructure • Critical services compromised • Health impacts/injuries to health responders
Tsunami	• Damage to facilities and/or critical infrastructure (in low-lying areas) • Impact on staff and families (physical, social, homes, transport, etc.)
Volcanic hazards	• Damage to facilities and/or critical infrastructure (within eruption and associated quake zones) • Ash impacts to water supplies, air quality, air-conditioning and facilities • Loss of staff (self-evacuating)
Wildfire	• Damage to facilities and/or critical infrastructure (in at-risk areas)

Step 3: Rate the likelihood and severity of hazards for the organisation

This step involves asking:

- What is the likelihood that a major hazard will occur?
- What are the potential consequences if it does?

Consider the consequences and likelihood for each of the identified hazards and use the simple ***risk matrix*** below to determine a threat level. Use common sense and available data to determine levels appropriate for the organisation's setting and locality.

Remember, even a relatively unlikely risk becomes important if its consequences would be catastrophic.

Template:
Complete column 3 ***Table 8: Hazards and risks***

Simple Risk Matrix

	Likelihood of occurrence		
Potential severity of impact	**Unlikely**	**Possible**	**Likely**
Major Significant impact on operations Threatens business continuity	**Medium**	**High**	**High**
Moderate Significantly disrupts short term operations	**Low**	**Medium**	**High**
Minor Inconvenient, no real ongoing impact.	**Low**	**Low**	**Medium**

Step 4: Rank the risks and make an informed decision about what action to take.

Revise the table so that the hazards with the lower threat are at the bottom, and those with the highest threat are at the top – these are the hazards which are the most threatening to your business and its operation.

For each of the critical business functions identified and ranked in the business impact analysis, options are needed to:

- reduce the likelihood and consequence of the disruption to the critical functions
- implement alternative functions and resources to be used following a business disruption
- activate plans to recover and restore normal operations.

This is dealt with in detail in the following section.

Business continuity options

By identifying and evaluating a range of business continuity options you will be able to select appropriate ways of:

- reducing the likelihood and consequence of disruption to critical functions
- implementing alternative activities and resources to be used following a business disruption
- recovering and restoring normal business operations.

The options selected should:

- provide for the resumption of functions at an acceptable level of operation and within acceptable timeframes.
- take into account any actions or strategies already in place within the organisation
- be based on the outputs of the business impact analysis and risk assessment.

In choosing the appropriate option or strategy, you should consider the:

- maximum tolerable period of disruption for each function
- cost of implementation.
- consequences of inaction
- key resources required, e.g. people, premises, technology, information, and supplies.

A useful starting point for choosing business continuity options is to consider the following scenarios:

- loss of access to premises.
- loss of or damage to facility
- shortage of staff/loss of key staff
- failure of technology
- failure of key supplier or partner
- failure of utility services

Template:
Complete ***Table 9: Business continuity options*** using the examples in Table 5 of this guide.

Table 5 below provides examples of how the information gained in the Business Impact Analysis can be used to develop the Business Continuity Plan.

After selecting appropriate business continuity options, identify the actions required to ensure that the options are implemented. Identify a timeframe for each action and who will be responsible for the follow-up.

Template:
Complete Column 3 ***Table 9: Business continuity options***

Table 5: Using business your business impact analysis for the business continuity plan

	Critical function requirements identified in ***Business Impact Analysis***	***Business Continuity Plan*** documents how the requirements can be achieved. Consider the following issues and strategies (not an exhaustive list) :
PEOPLE	• Key staff • Key skills • Expertise / competence required • Minimum staffing levels required to continue / recover key functions	• Management structure for dealing with an incident • Notification procedure / protocol • Information and advice to staff (response procedures) • Succession planning • Key staff / contact list (including out of hours details) • Multi skill training in key areas • Cross-training of skills across a number of individuals • Short-term replacements and training • Process mapping and documentation - to allow staff to undertake unfamiliar roles are • Reciprocal arrangements to cover staff short falls, backed by contractual agreements • Communication strategies – communication channels and messages for different groups such as staff, clients, external stakeholders, and the general public • Staff welfare issues and the psychological effects of the disruption on staff • Inventory of staff skills not utilised within existing roles • Other members of staff undertaking other non-specialist roles
PREMISES	• Key facilities • Key Equipment • Key Resources • Specialist Equipment • Security / restrictions • Alternative sites • Alternative facilities	• Loss / damage assessment • Site/facility security • Inventories of equipment/ resources and details of how to recover these • Salvage, site clearance and cleaning arrangements • Operate from more than one site • Are existing facilities multi-purpose? • Displacement of staff performing less urgent business processes with staff performing a higher priority activity. • Remote working – this can be working from home or working from other locations • Relocation arrangements / procedures for use of premises provided by other organisations • Alternative sources of plant, machinery and other equipment

	Critical function requirements identified in ***Business Impact Analysis***	***Business Continuity Plan*** documents how the requirements can be achieved. Consider the following issues and strategies (not an exhaustive list) :
PROCESSES	• Key processes • Critical periods • Key documentation / data • Record keeping requirements • Key communication requirements	• Copies / Back-ups / safe storage (recovery procedure) • Contingency procurement arrangements • Documented alternative (e.g. Manual) procedures • Data recovery procedures • Use of secure and fire-proof in-house storage facilities • Off-site storage of data • Continuity of protection of classified information / legal requirements and exposures • Affected decision-making processes • Action cards for recovery of key processes • Checklists • Alternative means of communication
PROVIDERS	• Key dependencies • Key contractors / providers / suppliers • Reciprocal arrangements	• Contact details for key providers / contractors / suppliers / support services • Alternative suppliers / providers / contractors (required for key functions) • Resilience capability of suppliers / providers / contractors to business disruption • Reciprocal arrangements in place with other organisations • Third party business continuity arrangements
PROFILE	• Key stakeholders • Legal / statutory / regulatory requirements • Vulnerable groups	• Communication strategy / plan / procedures • Systems to log decisions / actions / costs • Stakeholder liaison (regulator, clients, unions) • Media liaison • Public information / advice • Notification of at risk groups / alternative care arrangements

Responding to an event

This part of the plan contains checklists and other forms to guide action in the event of a major disruption or emergency. The purpose is to key personnel to provide an effective and timely response to ensure minimal disruption to operations in the event of a disruption. Response strategies need to consider three response phases:

- ***Emergency Response or Initial Incident Response*** - these strategies will be focused on the emergency response. However, it is essential to consider broader issues that may by impacted by a major incident such as communication with customers, stakeholders, financial impacts, community and political issues.
- ***Continuity Response*** - strategies during this phase aim to recover a minimal acceptable level of business operation. Continuity responses may include manual workarounds, replacing resources and equipment, outsourcing functions, and implementing alternative work processes.
- ***Recovery Phase*** - these strategies aim to return to a normal level of business operation. They may include obtaining additional resources to process the backlogs, validating or auditing activity during the disruption to ensure no errors have occurred and testing facilities and equipment to ensure full functionality after the disruption.

The plan should document the tasks that will be required to manage the initial phase of the incident and the individual responsible for each task.

One of the greatest challenges during and immediately after a crisis is thinking clearly. This is an ideal time for the use of a checklist to ensure that no major tasks are forgotten.

Consider the initial actions, after life safety issues have been dealt with, that the response team will need to focus on.

The template includes examples of the type of information, including checklists that can be included when planning a response to a critical incident. Text can be added to outline any arrangements already in place, including any specific actions identified for specific hazards.

Template:
Complete ***Table 10: Incident response checklist***

Activation: Declaring a business disruption event

Declaring the business disruption and agreeing on the appropriate time to initiate a response under the business continuity plan can be difficult and requires advance planning. There is a natural tendency for people to delay action until they are "certain" that an emergency is imminent or is serious enough to react. Therefore it is important to give clear guidelines on the declaration of a business disruption. A flow chart is useful for this purpose.

Template:
Document the procedure for activating a business continuity response.

The method by which a business continuity response is initiated should be clearly documented, setting out the individuals who have the authority to initiate a response and under what circumstances.

The plan should also set out the process for mobilising and standing down the relevant teams. In doing this, you should consider putting in place arrangements so that the relevant teams are mobilised as early as possible when an incident occurs.

Identify any injury and/or damage

As soon as possible, only if safe to do so, an assessment should be made as to the extent of the damage caused by the emergency. Consider, and document, the following:

- injury to staff, contractors, public
- damage to buildings
- damage to plant, equipment, vehicles
- damage to reputation.

Liaise with Emergency Services

If the Emergency Services are involved in the incident you will need to appoint somebody from your organisation to act as a Liaison Officer. This person needs to pass information between the Emergency Services response and your response team.

Evacuation Procedures

Appropriate evacuation procedures are needed that cater for both staff and visitors. These procedures should be stored in a place accessible to all staff and be tested on a regular basis.

You should identify a robust location, room or space from which an incident will be managed. Once established, this location should be the focal point for the organisation's response.

An alternative meeting point at a different location should also be nominated in case access to the primary location is denied. Each location should have access to appropriate resources, such as telecommunications, by which the incident team may initiate effective incident management activities without delay.

You should also have your "emergency pack" on site.

Emergency pack

If there is damage to the building or if it must be evacuated and operations need to be moved to an alternative location, an emergency pack can be picked-up and quickly and easily carried off-site. Alternatively it can be stored safely and securely off-site. This enables information and resources to be readily available during a business disruption event.

Template:
Customise and complete ***Table 10: Incident response checklist***

Incident Log

It is essential to keep a log of the actions taken and the decisions made, including the time, for later debriefing and review. Use the Incident Log to record information, decision and actions during the response period.

Template:
Start an ***Incident Log*** (Table 12) as soon as possible after a major incident.

Contact Staff & keep staff informed

It is essential to keep staff informed regarding the emergency and the response actions being taken. Staff may be concerned about:

- Colleagues who may be injured
- What's happening with their family?
- What is expected of them today
- Should they turn up for work tomorrow
- Will there still be a job for them if the building has gone up in smoke, etc.

Convene a Recovery Team

Identify a recovery team to assess initial disruption and losses and to begin a recovery plan. Make it clear who needs to do what, and who takes responsibility for each action.

Use the table below to assign responsibility for completion of each task for each designated role. Assign each role, or multiple roles, to one or more staff members and assign back-up staff as appropriate. The staff members involved should be given this table in order to understand their roles and as a task assignment list for completion of pre-emergency planning and emergency tasks. Customise the table to suit the organisation's needs and structure.

Template:
Complete ***Table 13: Emergency Roles and Responsibilities***

Identify functions disrupted and resources required

Document which functions or areas have been disrupted and the extent of the disruption. Start with the critical resources identified in Step 6 of the Business Impact Analysis, including people, facilities (including buildings and equipment), technology (including IT systems/applications), telecommunications, vital records and interdependent entities.

Template:
Complete ***Table 14: Record of disruption and resources***

Communication

The plan should set out the arrangements for mobilising the response team and for communicating with staff, wider stakeholders and, if necessary, the media.

Template:
Complete ***Table 15: Communication Strategy Checklist***

Communication is important to ensure that key stakeholders, employees and management are kept informed of the situation and changes over time. This will also assist in communicating to stakeholders any consequences that may affect them. There should be an up to date contact list and the location and method

of obtaining it described in the plan. Factor in the possibility of lost communication systems in a larger event.

Keep a communications Log to record all communications and decisions with resulting actions taken during the emergency.

Template:
Complete ***Table 16: Communications log***

Contact lists

All plans should contain or provide a reference to the essential contact details for staff, key stakeholders, partners and providers. If telephone communications are not available, consider collating a list of home addresses and distance (time) to travel for key staff.

Template:
Complete ***Table 17: Staff contact list***

Template:
Complete ***Table 18: External contacts list***

Use the table below to document external services (including Emergency Services) contact details. Each organisation will have different external providers and stakeholders.

All contact lists must be kept up-to-date and be readily accessible.

Recovery and maintenance of your plan

It is important to record and evaluate every major disruption or emergency. A debrief should be conducted as soon as possible after every major disruption. It is important to note that this is not a fault-finding process. It is critical to avoid criticism and blame

By analysing successes and failures, lessons to be learned identified and actions can be taken to improve business continuity planning and future responses. The Business Continuity Plan should be updated and key lessons learnt shared with all concerned.

Set a date to review the Business Continuity Plan

Returning to normal operations

A disruptive event is declared to be over when services have returned to 'normal' or at least a near approximation of the pre-event functioning. At this point the organisation can 'stand down' or deactivate their business continuity response, and return to the business as usual management structure. It is important to document this decision.

Exercising the plan and arrangements

The Business Continuity Plan cannot be considered reliable until it is exercised and have proved to be workable. Testing and rehearsing the plan provides the opportunity to test the arrangements and principles of the plan in a "safe" environment, without risk to the organisation

The frequency of exercises will depend on the organisation, but should take into account the rate of change (to the organisation or risk profile), and outcomes of previous exercises (if particular weaknesses have been identified and changes made).

Exercising should involve: validating plans; rehearsing key staff; and testing systems which are relied upon to deliver resilience. There are various levels of rehearsal or evaluation which can be used they vary with cost and value, however a planning lifecycle should allow for periodic tests of different types

A **discussion based** exercise is the cheapest to run and easiest to prepare This type of exercise brings staff together to inform them of the plan and their individual responsibilities It will involves a discussion of the plan to identify problems and solutions and is particular useful for training purposes It provides an important tool for embedding business continuity in the organisation's culture and as an initial validation of the new plan

A **table-top exercise** for small to medium sized organisations is likely to offer the most efficient method of validating plans and rehearsing key staff. Using a "what if?" scenario, this type of exercise engages people and can generate high levels of realism and provide participants with an opportunity to get to know the people with whom they would work in the event of a real incident

A full **live exercise** shows how well different elements in the plan work together A live exercise ranges from a small scale test of one component, such as evacuation or communications, through to a full scale test of all components of the plan While single component tests are relatively easy to set up, full tests are much more complex and can be expensive.

Whatever type of exercise is used, inviting stakeholders can be useful. It is also important to record and evaluate the event, through a debriefing immediately after the exercise and then documented in a lessons learned report with actions if required. The Plan should document:

Template:
Complete ***Table 19: Staff training record***

- how new staff are orientated to emergency management/Business Continuity procedures
- the programme for regular updates and refreshers
- the programme for exercising all, or elements of, the plan
- other relevant planning activities, e.g. DHB emergency exercises.

Reviewing and updating the plan

The plan should be reviewed and updated at regular intervals or when initiated by:

- changes to the organisation, including staff, restructurings, and model of service delivery
- changes to the external environment in which the organisation operates
- lessons learned from an incident or exercise

Template:
Complete ***Table 20: Review Checklist***

Any review should document and verify the checklist items.

Embedding competence and awareness

At its best, business continuity planning is accomplished by its integration into the very culture of an organisation This can be achieved through a combination of awareness raising and training Mechanisms for raising and maintaining awareness of business continuity planning with all staff include:

- involving staff in the development of the organisation's strategy
- written and oral briefings
- learning from internal and external incidents
- discussion based exercises
- including the strategy in the staff induction process

References and resources

Websites*:*

Ministry of Health (see Emergency Management) http://www.health.govt.nz
Ministry of Civil Defence http://www.civildefence.govt.nz
New Zealand Risk Society of Risk management. http://www.risksociety.org.nz

Documents:

Australian/New Zealand Standard (AS/NZS 5050:2010). Business continuity — Managing disruption-related risk. (*Describes the application of the principles, framework and process for risk management, as set out in AS/NZS ISO 31000:2009, to disruption-related risk).*

International Standard (ISO 22301: 2012) Societal security — Business continuity management systems — Requirements. (*Specifies requirements for setting up and managing an effective Business Continuity Management System).*

National Health Emergency Management Plan (see Ministry of Health Website –revision currently in development).

The National Hazardscape Report (2007). Officials' Committee for Domestic and External Security Coordination, Department of the Prime Minister and Cabinet, PO Box 55, Wellington, New Zealand.