Business Continuity Plan Toolkit

Contents

The Template – instructions for use 2
Introduction 3
What is the purpose of this toolkit? 3
Why do you need a Business Continuity Plan? 3
Step 1 Assign Responsibilities 4
Step 2 Analyse Your Business 4
Step 3 Identify Critical Dependencies 5
Step 4 Assess The Risks 6
Step 5 Develop Your Strategy 7
Risk Mitigation 7
Contingency Planning 7
Step 6 Develop Your Plan 8
Step 7 Exercise Your Plan 9
Step 8 Plan Maintenance 9

The Template – instructions for use

This document is designed to be used in conjunction with the electronic template which you can access from the Make a Plan button on the Be Prepared Toolbar. You can also download a blank copy of the template here.

To prepare your plan:

1. Use this toolkit to guide you through the steps required to build a Business Continuity Plan.
2. Once the arrangements have been agreed use the electronic template to create the documented plan.
3. Collect and prepare your information in advance. **Please note** *that the electronic template has to be completed in one sitting as it cannot be retrieved via the website once saved*.
4. Complete all of the relevant sections using the Previous and Next buttons to navigate through the input screens. You can leave sections blank when they are not appropriate.
5. When you have completed all relevant sections use the Build Our Plan button to create the final document.
6. Save the resulting document onto your local computer drive or another memory device. Please note that it will not be saved to any location other than the one(s) you select. For instance the website template will **not** automatically create a copy for LLR Prepared.

7. Your Business Continuity Plan will be created as a pdf document. You can print this document but you will need to convert it into a text format before you can edit it. This can be done through Microsoft Word 2013 or Adobe Acrobat XI Standard. If you don't have either of these you can send you pdf document to the Resilience Partnership Team using the Contact Us screen and we will convert if for you.

8. If you experience any problems when using the electronic template please send details to us using the Contact Us screen in the first instance.

Introduction

What is the purpose of this toolkit?

This document is a step-by-step guide to help you produce a Business Continuity Plan. The process of completing a Business Continuity Plan will help you prepare for business interruptions arising from any of a range of events.

This is a simplified template that has been designed for use by small or medium sized businesses to create a basic Business Continuity Plan. Other templates and on-line products exist that can be used for undertaking comprehensive Business Impact & Risk Analysis (BIRA) and continuity planning. We suggest you review a number of these before deciding which is best for you.

Together the toolkit and template are designed for completing a Business Continuity Plan from scratch. However, if you already have one, you could use them to update or validate your existing plan. You can use the template and toolkit as they are, alternatively you might tailor your approach to better suit the needs of your particular operation.

Why do you need a Business Continuity Plan?

Businesses become acutely vulnerable once they experience a disaster. The ability to respond quickly to protect reputation and to resume operations is vital to longer term recovery and viability - inevitably many businesses fail following a disaster. Business Continuity Management (BCM) is about identifying those parts of your organization that you can't afford to lose, then planning how to maintain these if an incident occurs. If you plan now, rather than waiting for it to happen, you will be able to get business operations up and running in the quickest possible time and thereby minimize loss of business to competitors and the loss of your customers' confidence in you.

This toolkit breaks the process down into a number of steps, each addressing a particular set of questions:

Step 1	Assign responsibilities	Who will be responsible for implementing BCM within the organization?
Step 2	Analyse your business	What are your organisation's key products, services and functions?
Step 3	Identify dependencies	What are the critical activities and resources required to deliver your key products, services and functions?

Step 4	Assess the risks	What are the risks that might give rise to business interruption?
Step 5	Develop your strategy	How will you continue to operate your critical activities in the event of an incident (loss of access to premises, loss of utilities, destruction of equipment etc)
Step 6	Develop your plan	What actions would need to be taken, by whom and within what timeframes?
Step 7	Exercise your plan	Have your staff received sufficient training to give you confidence that the plan could be successfully implemented?
Step 8	Plan maintenance	How often should the plan be reviewed and updated to ensure it reflects changes to your business?

Step 1 Assign Responsibilities

It is essential that BCM has the full support of senior management and this should be obtained from the outset. Experience shows that without this support it is difficult to instil a sense of value and ownership among the rest of the workforce.

It is also important that an individual or a team is designated with specific responsibility for managing and coordinating the process in order to maintain the activity levels, focus and motivation required.

For these reasons it is recommended that

- A member of the senior management board is nominated to be accountable for BCM
- An individual or team from within the organisation is appointed with responsibility for taking the programme forward
- Responsibilities are assigned for ongoing review and updating

Various service providers offer consultancy services and support. The Business Continuity Institute can provide further details.

ACTION **Complete Table 1 in the template with the names of those people within your organization who will be accountable for BCM at senior management level, for operational delivery and for ongoing maintenance.**

Step 2 Analyse Your Business

The process requires a clear recognition of those processes within your business which are critical to providing key products and services, and the resources needed to deliver them. This also recognizes that certain functions or processes can be suspended for a limited period of time without serious financial or reputational impact. A Business Impact Analysis (BIA) will help you differentiate between critical and non critical processes, providing the basis for your continuity planning.

Working through your organization, consider each department and the functions they perform to determine which should be designated critical for business continuity. The following questions will help with this evaluation:

- Is the process time critical? How long could it be suspended without significant impact?
- Would your customers experience delays to their service provision if this process was suspended?
- Is this product or service being provided in a competitive or regulated market?
- Does the income from this product or service contribute significantly to overall revenues and profit?

Ascribe a priority rating (1 – 5) to each function. The following definitions are provided for illustration but should be revised to reflect the time lines inherent in your business operations.

1 Essential service/function and time critical within 24 hours (Phase 1 recovery)

2 Essential service/function and time critical within 72 hours (Phase 2 recovery)

3 Essential service/function and time critical within 2 weeks (Phase 3 recovery)

4 Secondary function supporting core business

5 Housekeeping

ACTION Complete Table 2 of the template with the findings from the BIA, ranked in priority order 1, 2 and 3. Create a new entry for each business function, up to a maximum of ten entries.

Step 3 Identify Critical Dependencies

You now need to quantify the resources required over time to maintain critical activities at an acceptable minimum level of operation. This would normally be a somewhat lower level than optimum (normal business running).

For each function designated as Priority 1 determine the following resource requirements:

Staffing

How many staff would be required to reinstate a minimum acceptable level of operation?

Are there any specialist skills or levels of expertise required to undertake these activities?

Computer systems and communications

What IT systems, applications and services are required?

What communications infrastructure is required?

What information is essential and how is it stored?

Equipment

What plant, machinery and other facilities are required?

Does the process require specialist or bespoke equipment?

Supplies and third party services

Does the process rely on supplies or services provided by a third party?

What stock levels do you maintain and how long would they last?

Now complete the same process for those functions given a priority 2 rating.

Now complete the same process for those functions given a priority 3 rating.

ACTION Complete Table 3 by listing the dependencies for each critical function, entering details for a maximum of 10 functions taking them in priority order. Use this information to determine the resource requirements for supporting a minimum acceptable level of function.

Step 4 Assess The Risks

In the context of BCM a risk assessment looks at the likelihood and impact of the variety of risks that could cause a business interruption. By assessing these you will be able to identify where it is possible to implement risk reduction measures and where backup (contingency) measures are needed instead. You should focus your risk assessment on the critical activities and dependencies identified in steps 2 and 3.

The following risks are typical to most organisations but there may be others you should consider too:

- Loss of staff (including specific expertise) – consider illness, resignations, industrial action, transport problems
- Loss of systems (IT and telecommunications) – consider equipment failure, product defects, suspension of supplier support services
- Information loss – consider loss or corruption of electronic records, destruction or misappropriation of physical records (financial, contractual, other), also undocumented knowledge held by staff
- Loss of utilities – consider mains electricity, water, sewerage, landlines and mobile phones
- Loss of premises – consider denial of access (short term), damage or destruction of all or part or your site
- Loss of key supplies – consider supply chain failure, product defects, liquidation of supplier businesses
- Disruption to transport – consider severe weather, fuel shortages, industrial disputes

Next, consider the following questions in relation to the risks you have identified:

- Is there a higher or lower likelihood of this occurring?
- Do you have arrangements in place to prevent or reduce the likelihood?
- Do you have backup arrangements that could be activated to reduce the impact?

Use the risk matrix below to rank the identified risks, relative to each other, based on your estimation of the likelihood that the risk could occur and the impact on business operations if it does.

B Higher Impact Lower Likelihood	A Higher Impact Higher Likelihood
C Lower Impact Higher Likelihood	D Lower Impact Lower Likelihood

ACTION Complete Table 4 in the template to create a list of identified risks with their matrix scorings.

Step 5 Develop Your Strategy

Your BCM strategy should address the resilience of your business operations on two fronts; a) risk mitigation - taking proportionate action to reduce or eliminate identified risks and b) contingency planning – designing backup measures against risks that cannot be eliminated.

Risk Mitigation

Using the information from Step 4 determine what measures could be taken to reduce the identified risks. Give priority to those in cells A and B. The following lists cover just some of the options you might consider:

Staff	Cross training and multi skilling to reduce dependence on individuals Succession planning Documenting procedures
Technology	Holding spare kit (possibly older replaced items) Service level agreements for support and replacement of essential equipment
Information	Regular data back ups stored off site Scanning of physical records Fire proof secure storage of essential documentation
Utilities	Backup power supply (generator), a supply of analogue phones
Premises	Geographical separation of business operations across more than one site - this provides internal options for site sharing when one location is affected
Supplies	Stock holdings for essential supplies Multi sourcing of materials and identification of alternative suppliers Proof of business continuity capability for key suppliers

Contingency Planning

This stage is about developing the arrangements that can be activated at the time of an incident to reinstate your critical activities. For the purpose of this exercise it makes sense to work from a survivable worst case scenario – typically destruction of premises and materials and loss of some key staff. In developing a strategy to address the worst case scenario, the elements within it should satisfy lesser events too.

The solutions and tactics you adopt for your contingency plans should reflect the requirements identified in Steps 2 and 3. The following lists cover just some of the options you might consider:

Premises	Amalgamation on other premises occupied by the organisation Reciprocal agreements with third parties for shared use of premises, plant and machinery Recovery space contract with specialist supplier
Technology	Maintaining IT backup resources, either at another site or by agreement with a third party

	IT recovery contract with specialist supplier
Staff	Setting up home and remote working capabilities Use of third party services backed by contractual agreements Hiring contract staff (if training requirements are minimal)
Reputation	Communications plan for issuing information and reassurance in the event of business interruption

ACTION Complete Table 5a in the template with details of the operational capability that will be required during Phase 1 recovery and the solutions for doing so.

Complete Table 5b with details of the further operational capability required during Phase 2 recovery.

Complete Table 5c with details of the further operational capability required during Phase 3 recovery.

Step 6 Develop Your Plan

Your documented plan should contain the following details:

- The names / positions of those with authority to invoke and lead the plan
- Emergency contact details
- Designated roles and responsibilities (Coordinator, HR, Media/Comms, Operations and others)
- Action plan

The action plan should list the tasks required for the following elements of the response:

Invocation	The method by which the plan is invoked, identifying the individuals who have that authority and the location from which they will initially operate. These actions should include the process for mobilising the relevant teams.
Incident management	Addressing the incident at the business site. These actions are likely to include locating and accounting for those who were on site or in the immediate vicinity following evacuation, liaison with Emergency Services and insurers, communicating information to the management team and to staff.
Situation review	Assessment of the information available as to the extent of the incident and its impact on business operations, leading to the decisions about which contingency plans need to be activated.
Escalation / stand down	The process by which contingency plans are activated, staff deployed and stakeholders notified. Alternatively the stand down process.

ACTION Complete Table 6 of the template. This information will form the core of your Business Continuity Plan Document.

Step 7 Exercise Your Plan

Your Business Continuity Plans cannot be considered reliable until they have been proved to be workable and your staff are familiar with their roles. The process for achieving this should be broken down into achievable modules which build upon each other.

Validating plans	This can be achieved by conducting a **walk through** of the plan with representatives from the various departments within your organisation. This should be designed to give the opportunity for discussion of the arrangements in order to identify problems, solutions and potential revisions.
Rehearsing key staff	A scenario based **table top exercise** is likely to offer the most efficient method of providing your staff with the opportunity to fully understand their roles within the plan. It should be designed to bring the appropriate staff together and prompt them to take decisions as a scenario unfolds, in very much the same way they would in the event of a real incident.
Testing systems and processes	Various aspects of the plan will be testable as one off exercises. These include the following and there may be others: • System tests - backup systems and data • Communications tests – equipment and procedures • Plan activation process • Staff callout (telephone tree) • Activation of third party contracts and agreements
Scenario based exercise (or full test)	Full tests are more complex and may have costs attached. Indeed, you may need to consider whether your organisation has the capacity to run such an exercise without disrupting critical day to day operations.

It is important to evaluate each training and testing event through a proper debrief immediately afterwards. Record lessons learned and action any changes that are required.

ACTION Complete Table 7 in the template to create a schedule for training, testing and exercising your Business Continuity Plan.

Step 8 Plan Maintenance

It is important once you have put your BCM arrangements in place to ensure they are kept up to date. A maintenance schedule should be established to ensure that your plans are updated to reflect:

- Changes to your organisation (operational, structural, technology or staffing)
- External changes (supplies and suppliers, regulatory or commercial)
- Lessons learned from an incident or exercise

Reviews can be conducted either through formal audit or self assessment and should verify that:

- Priorities regarding key products, services and functions remain appropriate
- Arrangements are fit for purpose

- Maintenance and exercising schedules have been adhered to
- Identified changes have been implemented and change control procedures have been observed
- There is an appropriate level of awareness amongst staff

It is suggested that the plan is updated with detail changes on an annual basis and reviewed fully every two years.

ACTION Complete Table 8 in the template to create a schedule for reviewing and updating your Business Continuity Plan.