

This is a five-step guide to help you commence your business continuity plan.

**Step 1: Analyse your business**

**Step 2: Assess the risks**

**Step 3: Develop your strategy**

**Step 4: Develop your plan**

**Step 5: Rehearse your plan**

### **STEP 1 – ANALYSE YOUR DEPARTMENT**

This step, also known as business impact analysis, determines which area of your activities are crucial to running the business. Business impact analysis enables an organisation to focus its risk assessment on the mission critical activities of the organisation rather than conducting a traditional all risks analysis.

- a. **Mission Critical Activities**
- b. **Internal factors**
- c. **Singular problems to unique activities**
- d. **External influences**

#### **Mission Critical Activities**

To assess mission critical activities consider which operations are crucial to the running of your business. Using the grading system with 5 as the highest, I would suggest anything that scores 3 or more is essential.

<b>Grade on a scale of 1 to 5</b>	<b>What is essential to the running of the business?</b>
	Employees?
	Products?
	Services you provide?
	Location?
	Major Client(s)?
	Main Supplier(s)?
	Specialist equipment?
	Unique premises?
	Time sensitive processes?
	Shareholders?

## **Internal factors**

Consider the factors which influence the impact of an incident on your business. Try to establish where your business is at it's most vulnerable if an incident occurs.

### **Consider:**

- Staff
- Customers
- Suppliers
- Systems and processes
- Partnerships
- Buildings
- Shareholders
- Timescales

A sample list of questions for you to consider, as a starting point are as follows;

<b>Here are some questions to consider with regards to your staff:</b>	<b>Answer:</b>
Grade departmental importance - which department is most/least vital?	
When is the departmental function most essential?	
Which people are most essential and when? Consider appointments and timescales in accordance with agreed WCC response teams	
Do you have contact details at another location for all your staff and key employers? Are they up-to-date?	
Do you have a plan of who needs to do what in case of an incident?	
Do you have a crisis team?	
Have you nominated deputies for the members of the crisis team in case they are not available?	

**What if scenarios**

<b>Grade on a scale of 1-5</b>		<b>Define</b>	<b>Suggest preventative action:</b>
	If you could not deliver an order to a customer?	e.g. broken van	Tel No for hire firm
		e.g. road blocks	Alternative route
	If your staff could not get to work?		
	If your suppliers or customers could not get access to your premises?		
	If your IT system was damaged?		
	If your specialist machinery was damaged?		
	If your telecoms were down?		
	If you could not get access to your building?		
	If a vital order was delayed?		
	If you could not operate from your location?		
	If you are unable to pay your staff or fulfill contractual obligations? Think of reputation, not only the short term.		

### Worst case scenario

<b>What would be the worst-case scenario for your organisation?</b>	<b>Define</b>	<b>Suggest preventative action:</b>
How long before your business would be severely affected: hours days months		
Would it survive the disruption?		
Do you have insurance against this eventuality?		
Do you have copies of insurance papers off-site?		
How much can you afford to lose if unable to run your business for days weeks months		
What do you need to do to stay operational?		
Do all heads of departments agree that this is the worst-case scenario?		

### Singular problems to unique activities

An activity may be unique to your department or have a unique aspect due to its complexity. You may have to take some time to consider probable resolutions and any implications.

## **External influences**

What external factors are likely to affect your department during a crisis?

<b>Aspect affecting you</b>	<b>The way it's affecting you:</b>	<b>Preventative Action:</b>
Local community	Mixed opinion about what you manufacture	Community project/local help
Government	New legislation	Need to comply?
Transport	Disruption to public transport	Have a list of employees with their own transport/ organise shuttle bus/ organise accommodation etc.

## **STEP 2 – ASSESS THE RISKS**

Before proceeding to this stage, ensure a senior member of staff agrees with the business impact analysis. This stage should involve a senior member of staff and co-ordinators.

Risk assessment identifies:

- a. Internal and external threats, liabilities and exposure, including risk concentrations, that could cause the disruption, interruption of loss to an organisation's mission critical activities.
- b. The likelihood of an incident occurring: is there a concentration of risk in a particular area/task?
- c. How vulnerable an organisation is to the various types of incident.
- d. A basis to establish a risk appetite and risk management control programme and action plan.

For the purposes of risk assessment, it is also important to look at:

- e. Worst case scenarios
- f. What functions and people are essential and when

**a) Internal and external threats**

<b>Grade 1-5 most/ least prepared</b>		<b>Grade 1-5 least/most likely</b>
	Does your plan work if the power fails?	
	Does it work when there is a fire?	
	Does it work if you cannot gain access to the premises?	
	What if your customers/ suppliers cannot contact you?	
	What if your suppliers cannot get to you due to floods/ cordons?	
	What if your suppliers cannot get to you due to their problem - do you have alternative suppliers as a back up?	
	What if your employees cannot get to work for a few days in a row?	
	Does your plan cover criminal damage? Are you insured?	

**b) Risk concentration scenarios**

<b>Examples of risk concentration scenarios:</b>	<b>Yes/No</b>	<b>If yes, preventative action:</b>
Do you have a lot of expensive equipment in one room?		Extra security
Do you have a lot of crucial machinery in one area of the building?		Extra safety devices/ alarms

**c) How vulnerable an organisation is to the various types of incident.** Examples of possibilities to think about in terms of how different elements of your department will be affected in case an incident occurs

<b>How will your customers be affected?</b>	
If there are delays in delivering the goods/services?	
If it's a council-related incident, will this damage your reputation? Do you have a planned PR response?	
Have you reassured them that you have a business continuity plan in place? Is your Communications department aware of its content?	
<b>How will other stakeholders be affected?</b>	
Staff - have you assured them that you have a business continuity plan in place and that their jobs will be secure in case of an incident?	
Are your staff aware of the role they have to play in case of an incident?	
Suppliers - have you assured them that you have a business continuity plan in place and that you will be able to pay them on time in case an incident occurs?	
Shareholders?	
Local community?	
Business neighbours?	
<b>If you share your premises with other companies in the building:</b>	
What's the nature of their business?	
What will happen if you are denied access to the building due to another company's accident?	
Can you do anything to mitigate the risk from another's business?	
Does your landlord have a BCP?	
Is your landlord complying with their	

responsibilities under law?	
<b>How will your financial systems be affected?</b>	
Do you have financial company details off-site? Back ups of recent transactions?	
Do you have an extra copy of your chequebook ( if appropriate)?	
Will you be able to pay your staff/ suppliers?	
<b>Other issues to consider</b>	
Will you be able to get hold of your vital papers - do you have copy details of your insurance cover off-site?	
Do you keep staff trees/ lists off- site?	

**d) Risk appetite: how risk averse are you?**

Establish how long your business can bear functioning at reduced capacity and what level that is.

What needs to be done to make sure it can function at minimum capacity?

**Define your risk strategy.**

Remember that you can't prepare yourself against all types of incidents, however much you spend, but here is a selection of approaches you could take:

- Accept the risks - change nothing, e.g. close the office/ plant down for a while and have a disaster recovery plan in place to sweep up the damage and get your business fully operational after some time has passed after an incident.
- Accept the risks, but make a mutual arrangement with another business or a business continuity supplier to ensure that you have help after an incident. This business could be a competitor, but it is common that for business continuity purposes they become a 'buddy'.
- Attempt to reduce the risks, e.g. by for instance changing or ending 'risky' processes or by taking out insurance. Although do note that insurance provides financial recompense and support in the event of loss, but does not provide protection for brand and reputation.
- Attempt to reduce the risks and make arrangements for help after an incident

- Reduce all risks to the point where you should not need outside help, e.g. through implementing broad continuity management principles in case of an incident.

**e) What is the worst that could happen?**

What are the worst things for your department and how likely they are to happen? If you are prepared for the worst, then you can deal with incidents of lesser scale. This will also help you put in perspective how to develop your contingency plans and how to put preventative measures in place.

Consider:	Answer:
What is the likelihood of this happening?	
Does your plan cope with it?	
What can you do to prevent it?	
How much can you afford to lose if unable to run your business for days/ weeks/months?	

**f) What functions and people are essential, and when.**

Consider which departments, divisions and members of staff are essential to running the business. Experienced and multiskilled members of staff can be a vital resource, are you aware of everyone's skills, experience and knowledge?

What functions need to be covered during an emergency and thereafter? Are there any time sensitive operations or specialist procedures that need to be performed? Ensure that you consult with department heads and at 'ground level' to get a comprehensive analysis.

### **STEP 3 – DEVELOP YOUR STRATEGY**

From the beginning of creating the business continuity plan, aim to embed a business continuity management culture throughout the department to ensure that business continuity management becomes an integral part of the strategic day-to-day business as usual operational management. Achieve this by winning over middle management and building awareness that BCM is a council-wide responsibility not just an IT function.

As a guide each business continuity plan should aim to contain the following:

- a. **Statement of clear purpose of the plan**
- b. **The structure of the crisis team(s)**
- c. **Business recovery**
- d. **Work area recovery**
- e. **Technology recovery**
- f. **PR**
- g. **Staff focus**
- h. **A description of the premises**

#### **a. Statement of clear purpose of the plan**

The plan should outline the direction to take in the event of an incident. It should include a clear statement on how risk averse you are and you may want to include a statement on what your definition of a disaster is, for example: "any unwanted significant incident which threatens personnel, buildings, or the operational structure of an organisation which requires special measures to be taken to restore things back to normal".

#### **b. The structure of the crisis team(s)**

It must be clear when emergency plans are to be implemented and who has the authority to implement them. The plan should include all persons responsible for initiating the plan's implementation, both junior and senior.

It must be clear who is responsible for what in the plan's execution and who has the key roles. It must also be clear to whom everyone answers.

The team to be divided in accordance with the 4 response teams as previously agreed by the Corporate Management board

If you have nominated a team to create, co-ordinate and deliver the plan, it might be helpful to divide the personnel involved in the plan into three different categories:

- Strategic - the thinkers responsible for the strategy, such as the DMT.
- Tactical - the planners and co-ordinators that will deal with the tactical aspects of the plan. These will include a senior management team of experts within your business. They are involved in your BCM approach and specific planning and responsible for co-ordinating and directing the resources of the business to ensure that the plans are being properly implemented. Silver people will link with Gold and keep them updated on the developing situation.
- Operational - the doers who will be responsible for recovering/ restarting crucial business functions. They are responsible for ensuring that their specific business continuity plans are implemented. They take direction from the Silver people and keep them updated.
- You may decide that you will need a set of plans for each of the Gold, Silver and Bronze teams, or a set of different plans for different Bronze teams, such as a separate IT department plan, which will, for instance, include more technical jargon and specific data.

In your contingency planning, make sure that all levels of staff involved in business recovery understand the nature of threat and the importance of planning. Allocate a list of suitable locations where your Business Continuity team should meet, if an incident occurs. This should consist of a room on-site and a meeting room at your alternative fall back site.

If an incident occurs, meet with everyone from the Business Continuity team as soon as you can, probably after the first planned emergency procedures have been implemented, and then continue meeting every 24 or 48 hours.

### **c. Business Recovery**

Develop practices and procedures needed to mitigate risk and reputation if business operations have been affected. It includes the priority tasks that must be addressed if the business has to relocate and needs to communicate with clients and service providers during the period of disruption.

It is essential that such lists are updated regularly, at least quarterly, and preferably monthly, and they must recognise the likely availability of staff 'out of hours' and weekends and during holiday periods.

The members of the 'crisis team' should be supplied with a simple check list of the actions they must take during and after an incident. Using brightly coloured cards or paper is a cheap and way of ensuring that people know they are using the most up-to-date version. The lists should be accessible and available at all times and in several locations, electronically and in hard copy.

#### **d. Work area recovery**

This could be the key aspect of your plan. If you intend to work from another site, there are several options to consider:

- You might decide some staff can work from home temporarily.
- You might have made arrangements with another company to use their facilities.
- Use a 'hot site', also usually provided by a specialist continuity company, makes desks available within about 4 hours. This option is easy to rehearse, but relatively expensive.

#### **e. Technology recovery**

The council nowadays has complex IT, telecommunications and utilities' structures in place.

##### **Information Technology:**

It is imperative to keep [inventory lists of software and hardware materials](#), as well as your suppliers so that you can replace them immediately if needed. Customise inventory lists according to your needs. It is worth checking in advance if your insurance covers the replacement of damaged items immediately, or whether you need the insurance company's consent.

##### **Telecommunications:**

You may have the capability to access your telephone system remotely, from another site. Make sure all relevant programming is undertaken as soon as possible. Make a list of all the access numbers and keep them safely with all your important documents on and off-site.

##### **Utilities:**

In case of a utilities failure, make sure you have a list of all of your utilities' providers, their contact details and your account numbers. Make sure you have an 'old style' telephone handset which you can plug directly into a telephone socket. This has its own power source via the line and will not be affected by a power cut.

## **f. Public Relations**

The PR process can make or break a company's reputation. PR will influence how existing and potential customers, suppliers and all other stakeholders will react to the incident.

- Nominate a department contact and ensure that all staff know who it is. For resilience, make sure more than one staff member is nominated and if possible, that they have had some training in media handling.
- Consider the possible use of emergency instructions to staff. If it is a seriously disruptive incident and you cannot keep all your staff on site during recovery, it is essential to keep them well informed about progress.
- If appropriate, have a pre-prepared list of facts on the organisation's functions, safety record, etc.

## **g. Staff Focus**

Consult your staff when drawing up the plan. This will ensure that they feel part of the plan and will therefore be more willing to participate fully when something does happen.

Be sensitive how you communicate your plan: the phrasing 'essential staff' or 'vital departments' suggests that some of your staff aren't as important as others. Obviously, they all are, but some priority needs must be met.

Make sure that you have plans in place to take care of your employees once an incident does occur. Consider the following contingencies:

- Petty cash for travel home in case of evacuation
- Counselling

## **Damage Minimisation**

Remember that there is a common law duty to minimise loss and this requirement is often invoked under a contract of insurance. It therefore follows that expense controls should not be abandoned in the anxiety to make the business operational again.

#### **STEP 4 – DEVELOP AND KEEP DEVELOPING YOUR PLAN**

In the process of developing your plan, make sure you have consulted all the decision makers in the business and involved your staff. Also, make sure you use non-technical language when writing up the plan, making it accessible to all your employees.

Has your business continuity plan incorporated all the necessary components?

<b>Check your business continuity plan against the following:</b>	<b>Tick off</b>
Does your organisation have a clearly defined, up-to-date business continuity plan for its entire weakest links, mission critical activities and their dependencies?	
Does your plan reflect the most up-to-date business impact analysis and risk analysis?	
Does your plan clearly define the role of the accountable business owner of the plan? (This could be the MD, CEO or business owner...)	
Has your plan been approved and signed off?	
Is it clear who is responsible for the plan's maintenance?	
Is the plan regularly reviewed in terms of its mission critical activities by the agreed person, such as the legal rep?	
Does the plan establish a clearly predefined response if an incident occurs until the point of full operation?	
Does the plan clearly define how to recover critical activities within the specified time frame?	
Does your plan clearly define personnel roles, their accountability, responsibility and authority?	
Have you established an appropriate time frame for review of the plan?	
Does the plan provide and define clear aims and objectives?	
Are there clear instructions on how to use your plan?	
Does the plan contain a diagram of the business continuity management structure?	
Does the plan clearly state the appropriate responses according to the emergency?	
Do you have clear details regarding purchasing, expenditure, and authority?	
Do you have a list of contents?	

Distribution list?	
Glossary of terms?	

### **Developing your plan:**

The plan should be divided into tasks to do immediately following an incident and those thereafter to avoid confusion.

To develop the plan you should have input from a cross section of your organisation ensuring that you include all grades within the hierarchy. This is vital to ensure a practical and workable plan.

Large organisations often consult with outside organisations who may be able to provide assistance when drawing up the plan:

- Find out what information utility companies will need in case of an incident.
- What information will your insurer need from you? Please make sure that you create [inventory lists](#) according to your needs. It is worth checking in advance if your insurance cover will allow replacing damaged items immediately, or whether you need the insurance company's consent.
- Think of who else will be affected by your decisions: your customers and suppliers? Involve them if you can in the planning process. How will they want the information communicated if an incident occurs?

### **Technology Resources**

There are companies providing information back-up services. You can arrange them to collect data/ copies of information every day, week or month. Alternatively, you can store back ups at another site, at your buddy's site or at home.

Some organisations will want to give instructions over a central audio system to all employees, it is useful to have recorded messages for all types of incidents, including testing of fire alarm, but also instructions of what to do in case of an external incident.

It is also worthwhile having pre-prepared messages for relatives and next of kin, what to say to them over the phone, in person or in writing. This will be useful if some staff could not be found or taken to hospital for treatment etc.

## **STEP 5 – REHEARSAL AND STAFF TRAINING**

Once the plan has been developed, it has to be subjected to rigorous testing. Testing should be carried out in an environment to reproduce authentic conditions.

Although it might not be practicable to change premises for a few days, it might be a good idea to test operating at other premises with the key staff for a few hours. You may believe this is costly or unproductive but it is a practical investment for your company's survival: should an incident happen for real you will be better able to cope with it.

You may believe this is costly or unproductive but it is a practical investment for your company's survival: should an incident happen for real you will be better able to cope with it.

It is important to instill a culture of business continuity management awareness from the very beginning throughout the company. A truly effective BCP must reflect 'business as usual' management process and be driven from the top of the organisation. It should be clearly set out in the organisation vision statement that is fully endorsed and actively promoted by the Board or the Executive Committee.

It is vital to test the plan with all the appointed business continuity team persons to make sure each is fully aware of their own responsibilities. They should be given a copy to read through and to understand their own particular responsibilities. By training your team in the details of the plan they will be much more efficient at implementing it should the need arise, and they may well have useful feedback to give about their own area of company expertise.

It is also important to revise your plan regularly, to reflect staff turnover and updates in technology, for example. Assign the duty of updating the plan to a member of staff and make sure it is regarded as an important regular activity.

There are numerous ways in which you could test your plan. Here are a few simple examples:

- Paper-based exercises:
  - Read through the plan, questioning each action.
  - Test the plan using what if scenarios. (New pieces of information can be added as the scenario unfolds, in the same way that more details would become clear in a real incident.)
- Telephone Cascading
  - This involves testing your Staff Communication Tree: initiate the process of phoning or texting people at the top of the tree. Measure the time it takes for the last people to receive the message. This also allows you to test the whole communication structure (are there any people on the list who have left the company?).
- Full rehearsal
  - If it's carried out in similar conditions to a real incident, it will show you how the different elements of the plan fit together. This may be expensive,

especially if it involves changing sites, but planning will reduce costs and the efforts might pay off in the future.

**How often should the plan be tested?**

Your plan will need a review at least once a year and will need to be maintained and updated regularly by an appointed person(s). An exercise to test the plan should be held every 2 years linked to a general exercise to test the main WCC plan.