

## **Business Continuity Planning advice for Businesses with 50-250 employees**

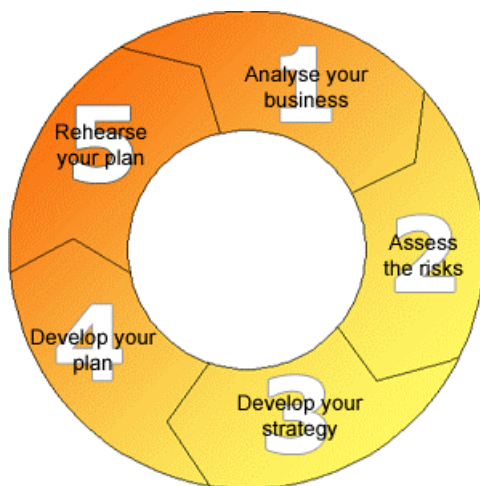
### **Where to begin?**

A business continuity plan should consist of a business and contingencies analysis. It needs to be developed by someone with an overview of the whole business, working with a team representing all the functional areas of your organisation, including approval and support from the very top.

Each plan will vary according to the size of the organisation, the nature of its business, and the complexity of location(s). You might need to create sub-plans for each department and then incorporate them into the total structure.

If your business is multi-layered or has a complex structure then you might want to use an external consultant for advice.

This five-step guide will get you started on business continuity planning. You can either use the interactive circle diagram or follow the page down to each section.



The steps are:

- [1. Analyse your business](#)
- [2. Assess the risks](#)
- [3. Develop your strategy](#)
- [4. Develop your plan](#)
- [5. Rehearse your plan](#)

### **Step 1. Analyse your business**

The first stage of business continuity planning is assessing which of the company's mission critical activities are crucial to running the business.

Approach the analysis by asking:

- 1) Where your business is most vulnerable
- 2) What would be the worst for your business.

With these questions in mind look at the following to see what needs to be planned and prepared to avert a crisis:

1. Staff
2. Customers
3. Suppliers
4. Systems and processes
5. Partnerships
6. Buildings
7. Timescales

### Checklists

We have prepared a series of checklists to assist with planning. The questions help assess the most vital parts of your business, and the weakest links. Grade your responses on a scale of 1-5, where 5 is the highest score and 1 the lowest. *Please note that these are examples only and you are strongly advised to customise the questionnaires according to your own company's needs.*

#### Mission Critical checklist

Grade on a scale of 1 to 5	Which are the mission critical activities? What is essential to the running of the business?
	Is it the people you employ?
	Is it the goods you sell?
	Is it the services that you provide?
	Your location?
	One major client?
	One especially good supplier?
	Do you use specialist equipment which is necessary to function?
	Do you have insurance cover in the event that you cannot gain access to your equipment?
	Do you have hire agreements in case you need to replace your equipment urgently?
	Do you operate from specialist premises that are hard to replace?
	Does your company rely on time sensitive processes?

#### Staff checklist

Here is a sample of questions to consider with regards to your staff:	Answer:
Grade departmental importance – which departments are most/ least vital?	
What equipment/ systems does each department need to function?	
When is the departmental function most essential, at a specific time of day or week?	
Which people are most essential and when? (Consider different timescales of a few hours, 24 hours, 5 days etc.)	
Are the contact details for all your staff	

and key employers lodged at another location? Are they up-to-date?	
Do you have a crisis team?	
Do you have a plan of who needs to do what in case of an incident?	
Have you nominated deputies in case the members of the crisis team are not available?	

Consider the following with regards to **outside influences** on your business.

<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 e.g. road blocks	Tel No for hire firm Alternative route
	If a vital order was delayed?		
	If your staff could not get to work?		
	If you could not get access to your building?		
	If you could not operate from your location?		
	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 your business partner fell ill?		
	If you became ill over a long period of time? Could someone else step in?		
	If you are unable to pay your staff/suppliers? Think of the company's reputation, not only the short term implications.		

#### **Worst Case scenarios**

<b>What is 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 all heads of departments agree that this is the worst-case scenario?		
Do you have insurance against this eventuality?		
Do you have copies of insurance papers off-site?		

## Step 2. Assess the Risks

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

There are three aspects to every risk to your business:

- [How likely is it to happen?](#)
- [How concentrated is the risk](#) (e.g. where a number of mission critical activities are located in the same area of a building/ same floor)?
- [What effect will it have on your business?](#)

### a. What if questions and checklists

Look at the following table and grade the responses on a scale of 1-5, 5 being most prepared and 1 being least prepared, as well as how most/ least likely the incident is to happen.

Grade 1-5 most/ least prepared	What if questions:	Grade 1-5 least/most likely
	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 customers cannot pay you?	
	What if your employees cannot get to work for a few days in a row?	
	Does your plan cover criminal damage? Are you insured?	

### Risk concentration scenarios

Examples of risk concentration scenarios:	Yes/ No	If yes, preventative action:
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

**What effect will an incident have on your business?**

<b>How will your customers be affected?</b>	
If there are delays in delivering the goods/ services?	
If you cannot contact them? Will they switch over to your competitors?	
If it's a company-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 PR 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 should 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 endeavour 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>	
Have you thought about working with your neighbours to create a joint business continuity plan?	
What's the nature of their business(es)?	
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?	
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 organisation lists and contact details off- site?	

**b) What is most likely to happen?**

Think about what the worst things for your organisation would be 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 insure your business, how to develop your contingency plans and how to put preventative measures in place.

**Worst case scenario**

<b>Consider:</b>	<b>Answer:</b>
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?	

**c) What functions and people are essential, and when?**

Make sure that every member of the business recovery team has details of their responsibilities and what they have to do in case of an incident. Make sure any information your staff keep at home for such a time is kept up-to-date.

**d) 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 are some strategies that are open to you

- **Strategy 1:** Accept the risks – change nothing, e.g. close the office/ plant down for while and have a disaster recovery plan in place to sweep up the damage and get your business fully operational some time after an incident.
- **Strategy 2:** 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'.

- **Strategy 3:** Attempt to reduce the risks, e.g. by changing or ending ‘risky’ processes or by taking out insurance. (Note that insurance provides financial recompense and support in the event of loss, but does not provide protection for brand and reputation.)
- **Strategy 4:** Attempt to reduce the risks and make arrangements for help after an incident
- **Strategy 5:** 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.

### **Step 3. Develop Your Strategy**

Although it is essential to perform business analysis and risk assessment prior to drawing up the plan, these components should not form part of the plan itself, but should be merely used as basis for formulating strategy.

From the beginning of creating the business continuity plan, **aim to embed a business continuity management culture** throughout the organisation to ensure that business continuity management becomes an integral part of an organisation’s strategic day-to-day business as usual operational management. Achieve this by winning over middle management and building awareness that BCM is a company-wide specialisation, 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\) A clear statement of support by senior management](#)
- [c\) The structure of the crisis team\(s\)](#)
- [d\) Business recovery](#)
- [e\) Work area recovery](#)
- [f\) Technology recovery](#)
- [g\) PR](#)
- [h\) Staff focus](#)
- [i\) 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” (*Definition taken from part 2, ‘How Resilient is Your Business to Disaster’, Home Office publication, 1997*)

#### **b) A clear statement of support by senior management**

To instil confidence amongst employees, it is vital that the plan is viable and will have the involvement and support of senior management.

### c) **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 could be divided as follows: Gold, Silver and Bronze personnel, and might include the likes of a chairperson, security, HR, media relations, transport, and finance and facilities .

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:

- **Gold** – the thinkers responsible for the strategy, such as the CEO.
- **Silver** – the planners and co-ordinators who 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 properly implemented. Silver people will link with Gold and keep them updated on the developing situation.
- **Bronze** – 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 threats 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, a place in a public building, e.g. a local pub, someone's house or 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.

### d) **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 checklist 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.

#### e) **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.
- Choose a 'cold site' agreement, usually provided by a business continuity supplier involves erecting a temporary building. You will usually be able to move in after about 12 days.
- Or 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.

#### f) **Technology recovery**

Most businesses nowadays have complex IT, telecommunications and utilities' structures in place.

**Information Technology:** It is imperative to keep **inventory lists of software and hardware materials**, (see the Checklists and templates page) as well as your suppliers so that you can replace equipment 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.

### **g) 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 company spokesperson, and ensure that all staff know who it is. For resilience, make sure more than one staff member is nominated and that they have some training in media handling.
- Make certain the story is the same from all sources: if the emergency services are involved, co-ordinate your information with them.
- Possibly hire a PR consultant.
- Consider the production of an emergency newsletter 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.
- Have a pre-prepared list of facts on the organisation's functions, safety record, etc.
- Place advertisements in local or national papers as needed.

### **h) 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 are not 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, such as petty cash for travel home in case of evacuation.

### **i) A description of the premises**

This is important for evacuation purposes. Clearly mark where the emergency exits are. Also, include lists of the contents of your premises for insurance purposes.

### **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. It could be worthwhile spending an afternoon brainstorming ideas. Use non-technical language when writing up the plan, to make it accessible to all employees.

When developing your plan it is worthwhile dividing it into **action immediately** following an incident and **action beyond the first hour** or so after an incident. (See the Checklists and Templates page for samples.)

#### **Who should be involved?**

Gold, Silver and Bronze personnel, including chairperson, security, HR, media relations, site manager, transport, for example.

Draw up a checklist of things that need to be done an hour after an incident, remember to include a list of practicalities and to create checklists according to your specific company needs.

There are some outside organisations who may be able to provide assistance when drawing up the plan:

- Find out from your local authority emergency planning officer what they would do in response to a major incident or terrorist attack.
- Keep in touch with neighbouring businesses. How can you help each other?
- Find out what information utility companies will need in case of an incident.
- Find out what information your insurer needs from you.
- Ensure that you customise **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.)
- Who else will be affected by your decisions: your customers and suppliers? Involve them if you can in the planning process and ask them how they want the information communicated if an incident occurs?

#### **Liaison with the emergency services and other organisations**

Talk to the local liaison officer of the respective **emergency services** to find out what their procedures are and what they will need from you if an incident occurs. Emergency services are often willing to visit companies and perform seminars on such subjects as evacuation procedures or safety to your employees.

The Fire Protection Association has published a useful guide: [“Safety at Scenes of Fire and Related Incidents”](#) which also covers problems of chemicals, biological hazards and building safety.

## **Cost**

Make an early assessment of the likely costs involved in creating and maintaining your plan, and budget for it. It does not need to be expensive, and many insurers will drop insurance premiums if you have a business continuity plan.

## **Staff training**

Make sure that you invest regular staff time into the formulation and maintenance of the business continuity plan. You should have the staff's commitment to make sure they will update all the necessary details and take the plan seriously.

## **Advantages/ Benefit of a Business Continuity Planning**

Developing a business continuity plan has numerous advantages, because it involves detailed business analysis. You might discover new, more efficient ways of doing things or notice existing loopholes that were difficult to detect earlier. It will also involve your staff who will have an opportunity to get to know the business better.

## **Step 5. Test your Business Continuity Plan and Train your Staff**

Once the plan has been developed, it has to be subjected to rigorous testing. You will never know if you have omitted something if you don't test your plan. The testing process 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. This 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 vital to test the plan with all the appointed business continuity team persons to make sure each is fully aware of their 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 area of company expertise.

It is also important to revise your plan regularly, to reflect staff turnover and updates in technology. 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 communications 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.

See the Checklists and Templates page for traditional types of BCP rehearsals.