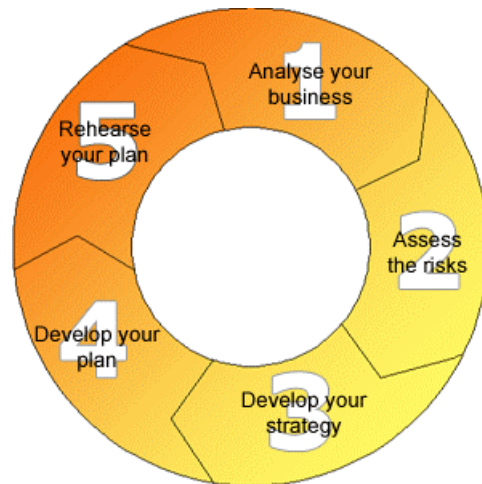


Business Continuity Planning advice for Businesses with 10-50 employees

Where to begin?

You can create an effective business continuity plan easily, in a relatively short space of time and for little outlay. This is a five-step guide to help small to medium-sized enterprises get started on business continuity planning.



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

This stage, also known as business impact analysis, deals with assessing which area of the company's operations (mission critical activities) are crucial to running business.

You should 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 topics to see what needs to be planned and prepared to avert a crisis.

- Staff
- Customers
- Suppliers
- Systems & processes
- Partnerships
- Buildings
- Timescales

Then, try categorising the information into mission critical activities by using the next steps to obtain a more detailed view.

You should end up with an overview of your business operations and a categorisation of all the processes/areas, highlighting that are essential to running your business.

Step 2. Assess the Risks

Before proceeding with this stage, ensure a senior member of staff/ board member agrees with the initial analysis in Step 1.

This stage should involve a senior member of staff and co-ordinators.

Analyse risk by asking the following questions:

- [How likely is it to happen?](#)
- [What effect will it have on your business?](#)

Before you look at risks in the individual parts of your business, think about what overall factors would mean a disaster. Any incident can become a disaster if it is not managed properly. If a business is correctly prepared for a disaster then a lesser incident should be easily managed.

What is the worst thing that could happen to your organisation and how likely is it to happen. Is there anything you can do to minimise the risk of it happening?

a) How likely is it to happen? Are you prepared?

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. *Please note that these are examples only. You are strongly advised to customise the questionnaires according to your company's needs.*

Grade 1-5 most/ least prepared	Scenarios	Grade 1-5 least/most likely
	Power failure	
	Building fire	
	Unable to access/leave premises	
	Loss of telecommunications	
	Flood/building cordoned off.	
	Suppliers' delivery or service problems.	
	Your customers cannot pay you	
	Your employees cannot get to work for a few days in a row	

b) How will your business be affected?

How will your customers be affected?	
If there are delays in delivering the goods/ services?	
If you cannot contact them? (Will they switch to your competitors?)	

If it's a company-related incident, will this damage your reputation? (Do you have a planned PR response?)	
How will other stakeholders be affected?	
Staff - Do they know that you have a business continuity plan in place and that their jobs should be secure in case of an incident?	
Staff - 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?	
If you share your premises with other companies:	
Have you thought about working with your neighbours to create a joint business continuity plan?	
What is 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 business continuity plan?	
Is your landlord complying with their responsibilities under law?	
How will your financial systems be affected?	
Do you have company financial details off-site?	
Do you have back ups of recent transactions?	
Do you have an extra copy of your chequebook?	
Will you be able to pay your staff/suppliers?	
Other issues to consider	
Will you be able to get hold of your vital papers eg. do you have copy details of your insurance cover off-site?	
Do you keep staff organisation lists and contact lists off-site?	

How risk averse are you?

Establish how long your business could continue to function at reduced capacity and what level that is. Consider how much you can afford to lose if you are unable to run your business for days/ weeks/ months.

I.e. should this reduced capacity be 50% operational, 20% operational, 80% etc? Is it better to close the office/ plant down for a while? Make sure you know your break-even point and what needs to be done to make sure the company can function at minimum capacity.

Remember, the impact of an incident on your business is likely to be a more pronounced affair than it would be in larger businesses. This might be because you are operating in specialised markets, have limited product ranges or relatively small customer bases. Therefore, any short interruption to normal working can have a profound effect, often halting output and leaving your customers in a helpless situation.

Step 3. Develop Your Strategy

What needs to be included?

Your plan should address the weakest links in your organisation and focus on the most vital aspects of your business. It should take into consideration worst-case scenarios having analysed their likelihood and suggested ways of minimising the risks of them occurring.

How do I formulate my 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 used as basis for formulating strategy.

Each business continuity plan should 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 statement should outline the direction the plan will take in case of an incident and include a clear statement on how risk averse you are.

It should include a statement of support by senior management to install confidence amongst employees and give the plan sufficient importance and authority.

You might find it helpful to classify what you consider to be a disaster within your statement, for example a standard definition may be: “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”, (*Taken from part 2, ‘How Resilient is Your Business to Disaster’, Home Office publication, 1997*)

b) The structure of the crisis team(s)

Everyone in your business should know when emergency plans should be implemented and who has the authority to implement it. The plans should specify all persons responsible for initiating their implementation.

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, or a place in a public building, e.g. local hall, 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.

c) Business Recovery

Develop practices and procedures needed to mitigate risk and preserve your reputation if business operations have been affected. Include the priority tasks that must be addressed if the business has to relocate, including communication with clients and service providers during the period of disruption.

Devise a strategy that prevents the worst from happening and minimises the effects of an incident.

Make sure that at this stage you have the answers for the following:

Considerations in developing your strategy:	Answer
What are the three most vital things to your business?	
What is the weakest link in your business?	

What are the three worst-case scenarios for your business?	
What effect will they have on your business?	
What preventative measures can you take to minimise the possibility of the worst happening?	
What measures can you take to minimise the effect it will have on your business?	E.g. prepare an off-site location to work from etc.

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 at weekends and during holiday periods.

The members of the ‘crisis team’ should be supplied with simple check lists of the actions to take during and after an incident. Using brightly coloured cards or paper is a cheap way of ensuring that people know they are using the most up-to-date version. The lists should be accessible 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 to use another company’s facilities.
- 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.

e) Technology recovery

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

IT: It is imperative to keep inventory lists of software and hardware, as well as suppliers so that you can replace equipment immediately if needed. (Please see the separate software and hardware inventory lists in the Checklists and Templates file.) 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: Make a list of all the access numbers and keep them safely with all your important documents on *and* off-site. Check whether you have the capability to access your telephone system remotely from another site. Make sure all relevant programming is undertaken as soon as possible.

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. You might want to acquire 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 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 that 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.
- If you cannot keep all your staff on site during recovery, it is essential to keep them well informed about progress.
- Place advertisements in local or national papers as needed.

g) Staff Focus

Consult your staff when drawing up the plan. This will ensure that they feel part of the plan and will be 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.

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

h) A description of the premises

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

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 two parts: **action immediately following an incident** and **action beyond the first hour** or so after an incident. (See the Checklists and Templates folder for templates.)

Some outside organisations may be able to help 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 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 among 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.

External help tools

Our suggestions and templates for plan development should be sufficient, but there are off-the-shelf plans available from bookstores or on the Internet.

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 that reproduces 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 in 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 members to make sure each has read the plan and 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 have useful feedback about their area of company expertise.

It is 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.