Expecting the unexpected

Business continuity in an uncertain world

National Counter Terrorism Security Office (NaCTSO) The National Counter Terrorism Security Office is a police unit working to the Association of Chief Police Officers, and provides a co-ordinating role for the police service in regard to counter-terrorism and protective security.

The unit collates and disseminates good practice and has responsibility for the management of police training in counter-terrorism protective security.

Developing and maintaining strong links with other organisations is a vital part of the unit's work, which allows for the identification of emerging needs and requirements in this area.

London First is a business membership organisation supported by over 300 of the capital's major companies. Its mission is to improve and promote London. London First's business members are in key sectors such as finance, professional services, property, IT, creative industries, hospitality and retail. Its membership also includes virtually all London's higher education institutions, as well as further education colleges, NHS trusts and independent hospitals. London First members account for 17 per cent of all employees in London and contribute 22 per cent to the capital's gross domestic product.

www.london-first.co.uk
Tel: 020 7665 1500

Business Continuity Institute The Business Continuity Institute's mission is to promote the art and science of business continuity management (BCM) worldwide. It provides an internationally recognised certification scheme for BCM practitioners and is involved in the development of international standards. Currently there are over 1,300 members of the institute working in 40 countries.

www.thebci.org
Tel: 0870 603 8783

Foreword

As Home Secretary with cabinet responsibility for the domestic security of this country, I am very pleased to support this positive initiative by the National Counter Terrorism Security Office, London First and the Business Continuity Institute. The key message of this booklet is the importance of planning and effective communication. We must be vigilant and well prepared and make arrangements to deal with the impact of a major incident or disaster. By remaining alert but not alarmed, we can reduce the ability of terrorists to carry out their threats. We cannot be complacent about the threat we face, but equally we all want to undermine the terrorists by continuing to trade, work and live in a free and tolerant society.

Business continuity and planning is just as important for small companies as it is for large corporations. Plans need to be simple but effective, comprehensive but tailored to the needs of the organisation. Employers have a responsibility to their staff for their safety and security, and we all share the desire to ensure that any disaster or incident – whether natural or otherwise – has a minimal effect on the economic well-being of the country.

I commend this booklet. I hope you will read it and act upon it. It is an excellent example of how, by working together and being proactive, we can protect ourselves, our livelihoods and our country. I wish this project every success.

The Rt Hon David Blunkett, Home Secretary

Expect the unexpected

Nearly 1 in 5 businesses suffer a major disruption every year. Yours could be next. With no recovery plan, you have less chance of survival.

How quickly – and painlessly – you manage to get back to 'business as usual' in the event of a terrorist attack, fire, flood or other natural disaster, or any other major interruption, depends on how effectively you can devise, and put into action, your own business continuity management.

Business continuity management can best be defined as:

'A holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.' (Business Continuity Institute, 2001.)

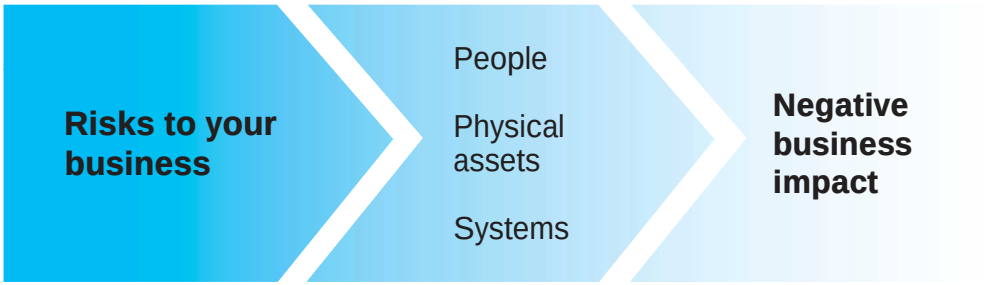
Building-in business continuity, making it part of the way that you run your business, rather than having to 'firefight' any emergency, helps prepare you to offer 'business as usual' in the quickest possible time. Planned business continuity management, so that your staff, customers and suppliers are reassured that you have an effective policy and practice for managing the unexpected, helps build confidence in your business.

Nearly 1 in 5 businesses suffer a major disruption every year. Yours could be next. With no recovery plan, you have less chance of survival.

Helping you to create an effective business continuity plan

This guide is the result of a unique partnership between the business community, police and business continuity experts.

Our aim is to provide you with a checklist and useful ideas on matching key business continuity management processes to your company.



Risks to your business

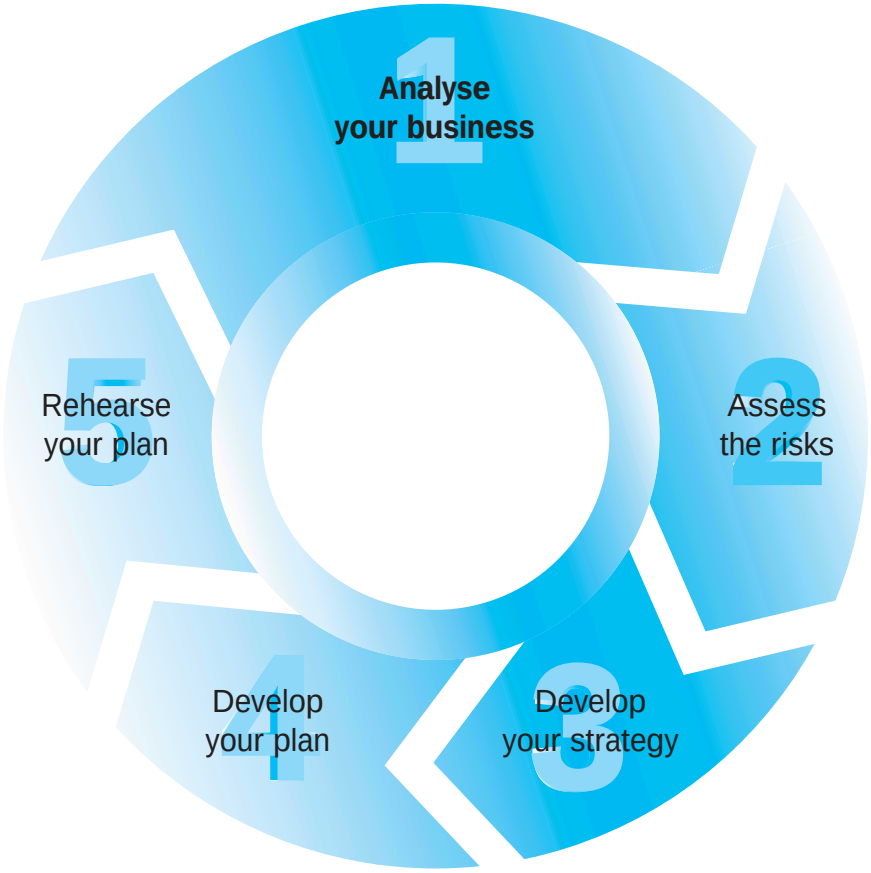
Without business continuity, a natural or man-made disaster could result in:

- Loss of work to competitors
- Failures within your supply chain
- Loss of reputation
- Human Resources issues
- Health and Safety liabilities
- Higher insurance premiums.

And, as every organisation knows, when setbacks arrive in combination, the worst case scenario can eventually be business failure.

Key steps in developing business continuity management

To help you match your plan to every step in your business' working processes, you may find it useful to follow these key steps.



1

Analyse your business

Step 1 is an up-to-date analysis of your business

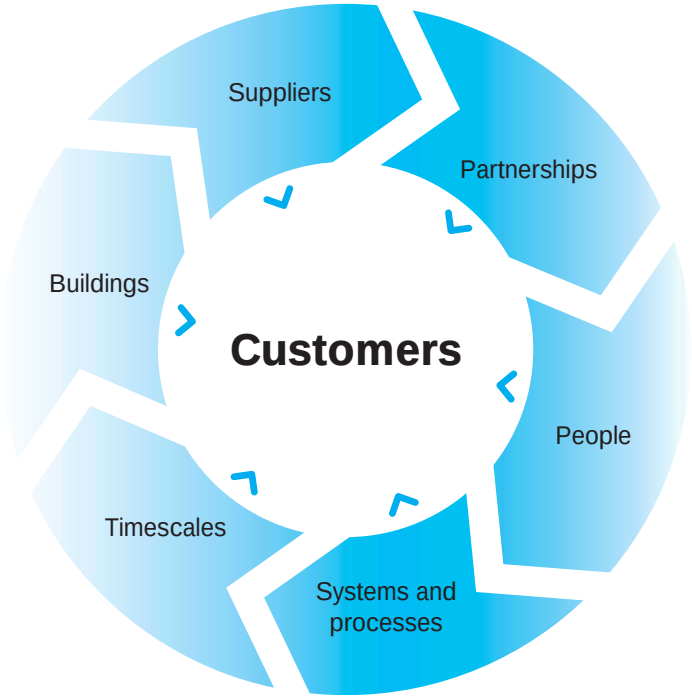
It is important that your Board and senior management know what you are planning to achieve. Arrange for them to watch the video-CD that accompanies this guide. It will help them understand why making your plan is important to the business.

It is also essential that your senior management fully supports business continuity management (BCM). Someone in senior management needs to have ownership of BCM. This means they need to be a 'champion' of BCM, from your planning work through to making sure everyone in your organisation adopts the results as normal business practice.

However well you understand your business, it will help to talk to other people

- You need the fullest possible picture of the complex interactions inside your organisation and between you, your customers and suppliers.
- You'll have the chance to help your colleagues understand why a business continuity plan is important.
- You want the people in your company involved. Knowing that their contribution is part of the planning and implementation process is important.
- You can include expert knowledge about every part of the business within your continuity plan.
- You can find out if any part of the business already has plans or procedures to deal with a major incident or terrorist attack. You'll need to include or adapt them in your plan for the whole business.

Where is your business vulnerable?



Checklist: who to speak to and why

The Board and Senior Management Team

- Have they seen the video-CD?
- Will they support BCM?
- Who will own BCM at a senior level?
- What do they agree is essential to the running of the business?
- What do they believe would be a worst-case scenario?

Heads of department

- How essential is the department's work to the running of the business? (Ask them to please be objective. This question is about practicalities, not profile.)
- What equipment, IT and other systems does the department need to be able to function?
- Who else inside or outside the business does the department need to be able to carry out their work?
- Who else in the organisation depends on this department?
- Who in the department is essential? (Again, ask them to be objective: the answer to this question may be about how one job fits in with another, not about how senior a manager someone is.)
- Are there any service level agreements, legal or regulatory obligations on the department?
- Do they already have business continuity plans for their department?

Facilities managers

- If your organisation has more than one site, each site will need its own business continuity plan, although they should all be based on the same principles. Find out from the facilities managers how each site operates.

Anyone else?

- Double check the practicalities. People who have keys, phone numbers, etc, may not work in the high-risk areas, such as IT, but your business cannot continue without them. Some vital people may not even appear on your payroll, for example your security team.

Assess the risks

There are two aspects to every risk to your business

- How likely is it to happen?
- What effect will it have on your business?

Business continuity management can help you balance them

You can define your assessment in cost terms: how much could you afford to lose if an emergency prevented you from doing business for days, weeks or months? How would suppliers, customers and potential customers react if your business received adverse publicity because you were unprepared for an incident?

There are three ways to work with the information you have gathered to provide an assessment of the risks.

a. Ask ‘what if?’ questions.
b. Ask what is the worst-case scenario.
c. Ask what functions and people are essential, and when.

a Ask ‘what if?’ questions

Remember that a good continuity plan will help your business deal effectively with an incident, no matter what caused it. You don’t have to be the target of terrorism for it to disrupt your power supply. Accidents such as workmen cutting through a cable or flooding from a ruptured water main could produce the same result: your building will have no electrical power.

Useful ‘what if?’ questions include:

- What if the electricity supply failed?
- What if our IT networks went down?
- What if our telephones went down? For a day? For a week?
- What if our key documents were destroyed in a fire?
- What if our staff could not gain access to the building for days, weeks or months?
- What if we had casualties?

It is also useful to ask ‘what if?’ questions about business relationships inside and outside the organisation.

- What if our customers could not contact us?
- What if our suppliers could not supply us?
- What if our customers could not pay us?
- What if we could not pay our suppliers?

Do not forget people issues: for example, after an incident, who will be responsible for recording who has been injured, where they have been taken and who is missing? How will you communicate after the incident? Who will deal with enquiries from the relatives of missing or injured staff? Do the staff, including temporary staff and contractors, know these details?

b The worst-case scenario

The second useful technique is to identify the worst-case scenario. If your plan enables you to cope with a worst-case scenario, it will also help you deal more easily with lower-impact incidents.

Your worst-case scenario will reflect what would be worst for your business. Generally, the worst case will be something that completely stops you carrying out your business. Think about cause and effect: a chain of events might be far worse than just one incident. For example: terrorist incident = no access to building = no access to IT system = customers unable to pay you = unable to supply your customers = bad publicity = damaged business reputation = a situation your competitors may be quick to exploit.

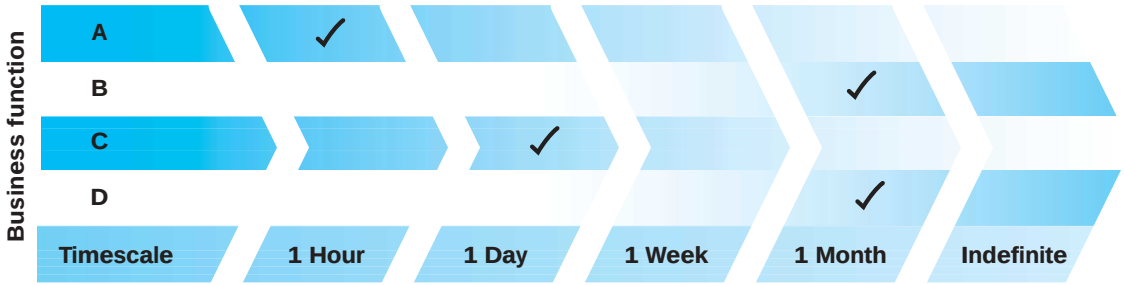
C What functions and people are essential, and when?

We all believe that our work is essential to our businesses. But, to make an effective business continuity plan, you need details of who needs to do what, when and where in the immediate aftermath of an incident.

You'll probably find it useful to keep a function/time matrix showing how quickly functions need to be up and running after a major incident.

Example of a function/time matrix

Some business functions will take longer to get working again. You'll have the details from the questions you asked in the first stage of making your plan. Your matrix can include details of when each person needs to be on site to restart functions that follow one another. Your plan should be flexible enough to cope with changes in urgency throughout the year. For example, how soon you need payroll services, or the processing of accounts, may vary depending on the time of year.



3

Develop your strategy

What is your appetite for risk?

First, double-check that the Board and senior management agree with your analysis of the business risks, and which people and tasks are essential. This will give you a clear understanding of the 'appetite for risk' within your organisation.

For example, one department may tell you it is essential to the business for them to be operational again within a day of any incident. It is up to the Board to agree if they are willing to accept the risk of that department not being operational again within the agreed time or if they would rather plan to reduce the risks.

Define your strategy

Whatever kind of business you are, you will probably choose one of the proven strategies.

These are:

- Accept the risks – change nothing.
- 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.
- Attempt to reduce the risks.
- 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.

Are you the kind of business that is committed to reducing risks, or one that prefers to take risks and have a 'comeback' plan? Your management's attitude to risk may be partly based on the costs of delivering effective business continuity. When working these out, remember to include both money and people's time.

*A business continuity supplier provides disaster recovery solutions to companies who are unable to continue business as usual due to an unforeseen disruption. Depending on the company, they can offer end-to-end service, from consultancy in the planning stages to the provision of all alternative IT and/or premises requirements.

A ‘hot site’ agreement: this is often provided by specialist business continuity companies who will normally have desks available within about four hours.

Working on another site

One essential decision is how you respond to risks that cannot be reduced, for example the risk of a terrorist attack destroying your building. How do you re-establish your business in another location?

- Make a mutual agreement with another company to use their facilities. This is an inexpensive option, but hard to rehearse.
- A ‘cold site’ agreement: normally a temporary building that can be erected on a suitable site, usually by a business continuity supplier. You will usually be able to move in after about 12 days. Again, companies who choose this option rarely rehearse it.
- A ‘hot site’ agreement: this is often provided by specialist business continuity companies who will normally have desks available within about four hours. This option is easy to rehearse but relatively expensive.

Your function/time matrix will include details of how quickly each department needs to be up and running. This will help you plan to have people in your temporary premises at the right time.

4

Develop your plan

Visualise your plan

Continuity plans should – and will – look different for different businesses. However, most good continuity plans share some important features.

Set-up

- Make it clear that you have consulted throughout the business.
- Use non-technical language that everyone can understand.

Contents

- Make it clear who needs to do what, and who takes responsibility for what. You should always include deputies to cover key roles.
- Use checklists that readers can follow easily.
- Include clear, direct instructions for the crucial first hour after an incident.
- Include a list of things that do not need to be thought about until after the first hour.
- Agree how often, when and how you will check your plan to make sure it is always a ‘living document’. Update your plan to reflect changes in your organisation’s personnel and in the risks you might face.
- A good plan will be simple without being simplistic. You will never be able to plan in detail for every possible event. Remember that people need to be able to react quickly in an emergency: stopping to read lots of detail may make that more difficult.
- Plan for worst-case scenarios. If your plan covers how to get back in business if a flood destroys your building, it will also work if one floor is flooded.

Matching your plan to your people

It can be useful to use the Gold, Silver and Bronze (GSB) structure to help define who should do what.

Gold

This usually refers to the CEO or other senior managers who make strategic decisions about the business, and who will also take strategic responsibility for responding to an incident, for example speaking to the media about the incident. ‘Gold’ people will communicate strategic business decisions following a terrorist attack or other major incident directly to ‘Silver’ people.

Silver

Usually a senior management team of experts within your business. Already involved in both your overall BCM approach and specific planning. They are responsible for co-ordinating and directing the resources of the business to ensure that the plans are being properly implemented. ‘Silver’ people will link directly to the ‘Gold’, keeping them updated on the developing situation.

Bronze

Identified in your business continuity plan as responsible for recovering/restarting crucial business functions. They are responsible for ensuring that their specific business continuity plans are implemented. They take direction from ‘Silver’ people and keep them updated.

You can apply the GSB approach to any business. It is essential for Gold, Silver and Bronze levels to have access to robust, working communications to ensure the proper co-ordination of business continuity plans.

You may decide that the size or structure of your organisation makes a set of plans – one for Gold, one for Silver and one each for the Bronze teams – more useful than one large plan. For example, your IT department may need a plan in a different format to include more technical information about their systems.

Include information from outside your business

No business operates in a vacuum. Include information from outside experts in planning for emergencies, or from other business people who face similar risks.

- **Emergency Planning Officer:** find out what your local authority would do in response to a major incident or terrorist attack.
- **Emergency services:** ask the fire brigade what they will want to know from you during a major incident? How can you help the ambulance service to help you? Who will the police contact at an incident? Ask about access to your premises if cordons were set up, for example.
- **Neighbouring businesses:** would a major incident on their premises affect you and vice versa? How can you help each other?
- **Utility companies:** telephone, electricity, water, gas. Find out what they will need to know if your business is involved in a major incident.
- **Suppliers and customers:** how will you contact them to tell them you have been affected by a major incident?
- **Your insurance company:** what information do they need from you? Do you need their permission to replace damaged critical equipment immediately.
- **Your customers and suppliers:** who will be affected by your decisions? Involve them if you can.

Use consultation as a PR tool

When you consult with other businesses, customers and suppliers, make the most of the opportunity to present your company as:

- An organisation that takes business continuity seriously
- An organisation that has a tried and tested plan, with management support and staff buy-in at all levels
- An organisation that will be able to be ‘back in business’ in the quickest possible time.

Rehearse your plan

Your plan is a living document

Sometimes, you only discover any weaknesses in a plan when you put it into action. Rehearsal helps you confirm that your plan will be connected and robust if you ever need it.

Remember your business continuity plans are ‘living documents’ and you will all need to rehearse whenever you update them. Rehearsals are also good ways to train staff who have business continuity responsibilities. You can also rehearse without disrupting people’s work.

Possible ways to rehearse your plan

- **Paper-based exercises:** read through the plan as a group, questioning each action. Is it the right thing to do? Does the plan ask you to do things in the right order? Then, test your plan using a ‘what if?’ written scenario. 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**: without warning, a test message is sent out to everyone at the top of the call cascade lists in the plan(s). The message is cascaded, with the last person in each cascade contacting a nominated person, who records when the calls come in. This allows you to check your communications structure. Are you having difficulty contacting people? Are the telephone numbers right? Are they still with the company?

- **Full rehearsal**: a full rehearsal will show you how well different elements in your plan work together, which may not be clear when you test the individual parts. This can be an expensive way to test your plan routinely, but planning should help you check the full plan with the minimum of cost and disruption.

Remember – in an uncertain world, you owe it to yourself to be an organisation that is confident of being ‘back in business’ in the quickest possible time.

For more information:

Business Continuity Institute: www.thebci.org

Home Office: www.homeoffice.gov.uk

London First: www.london-first.co.uk

London Prepared: www.londonprepared.gov.uk

Metropolitan Police Service: www.met.police.uk

UK Resilience: www.ukresilience.info

With thanks to the following London First members for their knowledge and expertise:

BT Group plc

DTZ Debenham Tie Leung

Ernst & Young

KPMG

Morley Fund Management

Prudential plc

Shell

Tesco plc