

**BCM Lite** – a quick and easy guide to BCM for beginners and/or small businesses

## Some important definitions

**Business Continuity Planning** – The process leading to a clearly defined and documented plan for use in the event of a serious incident that impacts the people, functions and/or reputation of the business. For example, loss of Head Office, virus attack, fuel crisis or product recalls.

**Disaster Recovery** - The process of planning your response to an incident that may result in a serious loss of IT systems.

**Business Continuity Management** - The overall management programme, by which all plans are developed, reviewed, maintained and exercised.

**Crisis Management** – The management of the specific incident at the actual time of its happening; in particular how communications are handled during the incident.

## Introduction

Ensuring that your company is able to respond to any event that might cause disruption to normal operations or damage your reputation is all about **being prepared**. Examples of such events include power failures, IT virus attacks, fire, strikes etc. Business Continuity is the management process through which your preparation can be achieved.

If you are able to satisfy the needs of your staff and customers (and other stakeholders) in the event of a major disruption you will undoubtedly increase the likelihood of your company's survival and will probably enhance your reputation by meeting the unexpected challenges that will arise.

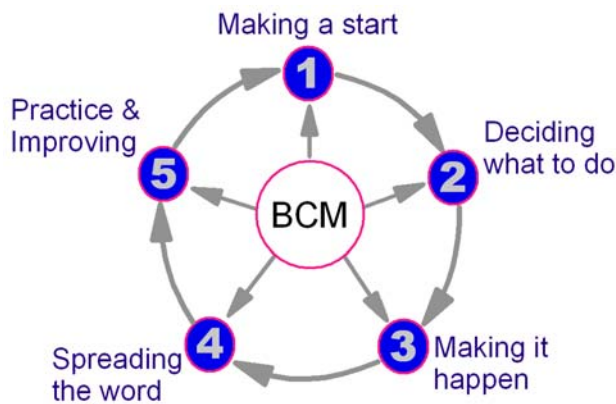
There are many real benefits to having a business continuity plan (BCP). These include:

- Confidence in the ability of your business to survive an unexpected catastrophe
- Demonstrating duty of care to your employees
- Ability to meet your customers' expectations in a wide range of circumstances and show due diligence to your company's other key stakeholders
- Safeguarding your company's reputation
- Competitive advantage gained due to a swift and effective response (you may be up and winning orders ahead of those unprepared and still affected)
- Early warning of, and corrective action to, any weaknesses or vulnerabilities in your business
- Potential improvements in your insurance costs and coverage
- May assist you in meeting certain legal and regulatory requirements.

And..... it's not as difficult or expensive as you might think!

This guide is designed to take out all of the complexity and jargon that can so often be associated with the development of a business continuity plan.

To develop your own BCP there are five simple steps to follow:



1. Making a start
2. Deciding what to do
3. Making it happen
4. Spreading the word
5. Practicing & improving

By using this 'keep it simple' approach, you can create a business continuity programme that suits the needs of your business and is also easy to maintain.

## 1. Making a Start

All of the current best practices for developing a BCP have been incorporated into this guide but with a focus on **keeping it simple and practical** so that it is easy to do.

The first step has to be an acceptance by the boss and the senior managers that this is a useful process. There are plenty of arguments for doing business continuity management and some of these are listed above; after deciding that these are benefits you'd like for your company then you are ready to start!

An overall co-ordinator for business continuity should be appointed to report directly to the boss or senior management team. This person is ideally someone who understands the business structures and people, has good project management, communication and interpersonal skills and is a good team leader. However bear in mind that the aim is to ensure that thinking about business continuity is part of every employee's normal responsibilities. Also remember that business continuity is not just the preserve of the IT department, although they will have an important role in planning and executing your recovery.

The BC co-ordinator (and team, if you are a large enough enterprise) provide the resource to manage the implementation of the BC programme throughout the organisation and to be in a state of readiness to guide the organisation in the event of a disruption.

## **2. Deciding what to do**

### **What do you want to achieve?**

In this stage the requirements of the Business Continuity response are discovered. They provide the basis upon which all subsequent BCM policies and processes are based.

The 'policy' questions to be asked are:

- What sort of disruptions do you expect the plan to provide a response to?
- Is anyone (e.g. Insurers, customers or regulators) imposing any specific requirements on your plans?
- Are there any imminent changes to the business to be taken into account?
- What sort of hazards is the business exposed to?

### **How long can you last without each part of your organisation?**

Everything that you do can tolerate a certain amount of interruption. Unless you run a 24x7 operation the business can clearly cope with interruption each night and at weekends; even continuous processes have maintenance breaks. You need to look at each operational department in your business and estimate how long you could do without it before it impacted the organisation to the extent it could put you out of business. This could be because customers will become fed up with your performance, cashflow seriously affected, your reputation becoming irreversibly damaged or the backlogs will get out of hand. These impacts will be minimal to start with, and then increase quickly as the disruption is prolonged.

If you have the time you could look inside each department and you will find some operations are more urgent than others. Again try to estimate the timescales and note the resources they require. Don't worry about the accuracy of your time scales. As you will see from the next section, there are a limited set of options for continuity.

Note the dependencies of functions on other areas - the urgency and resource needs of the organisation's internal departments (e.g. IT) are mostly determined by the urgency of the operational departments they support. Take particular note where you rely on the timely operation of a supplier since the impact of their failure may have disastrous consequences on your ability to deliver.

### **Minimising Risk**

On completion, this analysis enables you to focus risk assessments on the most urgent business processes and their infrastructure. You should consider measures that could reduce the likelihood or impact of a range of serious events.

### **Setting the scope**

The information you have collected above provides the information from which to choose an appropriate strategy because it identifies how quickly the loss of each part of the organisation would cause serious damage. An appropriate strategy can then be chosen to allow each function to be recovered before the time that the damage will occur.

Potential scoping strategies include:-

- Deciding whether or not you need an alternative site? If so then this should be an appropriate distance from your main site - several miles is likely to ensure that most incidents do not affect secondary sites - but the further you have to travel, the more disruption this will cause to displaced staff.
- Deciding how much you can afford to spend
- Deciding how much you could afford to lose.

### **Choosing the strategy for what you *do***

You need to work out how, and where, you might be able to resume business. You could:

- **Do nothing** – for the parts of the business that you can do without for many weeks.
- **Decide how much time you need before you have to start up at another location** – develop a plan to relocate to a prepared alternative location when resumption is required within days.
- **Split locations** – operating permanently from two or more geographically dispersed locations when resumption times are measured in minutes and hours will mean that you are able to simply switch to the other location if one goes down. This is particularly appropriate for retail organisations such as banks and shops.
- **Changing or ending the process** – deciding to alter or even end a business process in the event of disruption (for example : replacing a manufacturing process with subcontracting, importing and distribution).
- **Ignore the risk** - which will leave your organisation vulnerable to the impact of unexpected loss of facilities which may result in its closure.

Note that an inadequate strategy will only give you a false sense of security.

### **Choosing the strategy for what you *need***

To implement the strategy you may need to use external resources such as office space if the incident has rendered your site unavailable. Standby offices are available on a subscription basis or you could hope to find something suitable when the incident happens such as serviced offices or sharing offices with a partner organisation.

You should also look at:

- **Information back-up strategies** - to ensure your data is accessible even if your site is not
- **Insurance** – provides financial recompense for the additional costs of the resumption
- **Loss Mitigation** – practical procedures to eliminate / reduce risk (e.g. smoke alarms, sprinkler systems, anti-virus software etc.) - however this should not be at the expense of the business continuity planning effort - risk measures can fail!
- **Salvage Plan** – measures to minimise physical damage for example through the use of document recovery services, fire proof cabinets etc.

### 3. Making it happen

Once you have decided what to do you need to document it in a form that can be used when an incident arises. You must also structure your plan and staff so that each is focussed on an aspect of the response. A suggested structure is:

#### **Crisis Management Plan**

This is your immediate response to the incident, (which could be an operational blip that causes a loss of reputation or a fire that has damaged part of your facility or any other number of incidents). It's a plan for what you say to the various parties and how you say it, for instance your staff may need reassurance and direction as to what to do next.

The focus should be on managing the big issues for the organisation and coordinating the communications. As a minimum the crisis management plan should contain:

- A contact list
- Key messages.

#### **Business Continuity Plan**

The BCP provides the tactical response to the incident and resuming the business.

The BCP may include the following:

- General Introduction and overview
- Plan implementation
- How to maintain service continuity
- How to achieve service recovery
- Team structure and members and contact lists
- Communications plan for dealing with your various stakeholders.

#### **Incident Response and Business Unit Plans**

- An incident response team usually lead by a Facilities department who deal with the specific incident and its physical impact (if any)
- A Human Resources response to welfare issues in an incident
- Departmental resumption plans
- An IT recovery plan.

#### **Plan Structure**

The various plans should detail the response expected of each team during the following phases of the incident.

##### *1. First actions*

This involves the stabilising of the situation following an incident. It is useful to understand in advance the role, responsibilities and powers of the emergency services.

##### *2. Incident Management*

Bringing the situation under control:

- Communicating with staff, customers and other stakeholders and the media
- Making strategic response decisions.

### 3. *Business Resumption*

The procedures to resume business processes:

- Identify tasks to be undertaken by the business continuity team and business unit teams
- The teams required to perform required tasks and their responsibilities
- Identify key contacts, suppliers and resources
- Procedures for the recovery of information and documentation
- Telecommunications requirements for resumption
- Staffing requirements to deliver the agreed level of service.

## 4. **Spreading the word**

A plan will not work if people do not know what to do, or do not have the skills to do it.

Consider what skills you might need in an incident, for example:

- Media training
- Incident management.

Consider what you and your staff may need to know, for example:

- Evacuation plans and assembly points
- Procedures for resuming business.

Draw up a plan of training and awareness to make sure these stay current.

## 5. **Practice and improving**

### **Exercising the Plan**

Once you have plans it is important that they are exercised regularly to:

- Make sure they still work
- Make people aware of the role they play
- Test the readiness of external providers.

Rehearsals don't have to be hugely disruptive, you can rehearse different parts of the plans separately, or different departments at quiet times. The most important thing is that your staff have confidence in the plans and that they become workable and useful.

### **Keeping it up to date**

The plan may need to be amended to address:

- Errors that were identified during a rehearsal
- Recent changes to the business
- New requirements from customers
- Changing legislation.

### **Plan Audit**

An audit is an impartial review of the plans. It may be useful to get a qualified BC practitioner to check your plans against published standards and as a sense check. However you should never be tempted to get a consultant to write the plan for you since the learning is in the planning activity - not the plan itself.

**Other useful sources of information**

**The Business Continuity Institute - <http://www.thebci.org/>**

**Continuity Central - <http://www.continuitycentral.com/>**