White paper

ICM COMPUTER GROUP

Beginners Guide to
Business Continuity

BUSINESS CONTINUITY
Delivering business availability

Contents

Introduction

While bombs, fires and floods capture the headlines, almost 90% of crises are nowhere near as dramatic. It is these quiet catastrophes that have the potential to damage your organisation's most valuable assets; its brand and reputation. These can be destroyed very quickly unless strongly defended at times when the speed and scale of events can overwhelm normal operational and management systems.

Recent research has suggested that on average 20% of all organisations will experience some form of unplanned event once every five years. Whilst it is unlikely to be as catastrophic as 9/11, there is still the need to think about how you would cope with the more mundane events, such as power cuts or transport problems.

Who does it concern?

The fact that organisations are now so dependant on their IT systems has meant that during the last 20 years the IT department has led the way in planning how to recover from an unplanned event. But restoring data and system access is not enough when there is nowhere for employees to answer the phones or suppliers cannot deliver critical components. Incidents as simple and common as an extended power loss, telecoms failure or the loss of building heating may cause critical business functions to be disabled.

All of these are outside the scope of the IT department and impact all aspects of the organisation. So the short answer is: it concerns every department of every organisation – it is not just an IT issue.

Business Continuity Management

The options for dealing with an unplanned event include:

- Doing nothing
- Taking out insurance
- Preparing a business continuity plan

Whilst the first of these is the easiest and most common option it is not recommended for obvious reasons. The second can appear attractive, but will not cover you for events such as lost customers. So in the long-run preparing and testing a business continuity plan makes good economic sense.

Traditionally disaster recovery (DR) has been the start and finish of organisational strategy for dealing with an unplanned event. This would ensure that IT systems and data can be restored after unscheduled downtime. But over the last few years the growth of Business Continuity Management (BCM) has meant a shift in focus to the prevention of such events, rather than the cure of DR. This has meant that DR has now become a subset of the whole process.

BCM covers the whole lifecycle of disaster prevention and recovery. Although the initiative usually originates from IT, BCM embraces the entire organisation. It provides a planned and controlled method of anticipating and responding to events that are likely to interrupt key business activities.

Putting in place a BCM plan will help you to:

- Avoid financial losses
- Meet legal requirements
- Avoid loss of market share
- Protect the safety of assets including employees
- Mitigate negative publicity

Why organisations need business continuity planning

The speed with which modern business is transacted means that a disruption of only a few hours can have a catastrophic impact on the profitability and reputation of the affected organisation. Although this will have an immediate and adverse impact, it can also damage the long term viability of the organisation as well.

Recent research on the impact of an unplanned event has revealed some worrying trends. One in five of all organisations will suffer fire, flood or storm, power failures, terrorism and hardware or software disaster. Of those without a business continuity plan:

- 43% will never reopen
- 80% will fail within 13 months
- 53% of claimants never recoup the losses caused by the disaster
  (Source: Aveco)

- 90% of businesses that lose data from a disaster are forced to shut down within 2 years of the disaster
- 50% of businesses experiencing a computer outage will be forced to close within 5 years
  (Source: London chamber of commerce)

- Major systems downtime costs 15% of organisations over £50,000 per hour
  (Source: Information age)

Types of disaster

It is important to bear in mind that it is not only a catastrophic disaster that can adversely impact your organisation; even the most minor occurrence can have a potentially costly effect. These include:

Serious information security incidents – This covers events such as: cyber crime, loss of records or data, accidental or deliberate disclosure of sensitive information, and IT system failure. According to a recent DTI survey the average cost of an organisation's most serious security incident is £10,000, but for larger organisations this was more likely to be £120,000
Equipment or system failure – Includes: internal power failure, air conditioning unit failure, production line failure, cooling plant failure, equipment (excluding IT hardware) failure
Loss of utilities and services – Electrical power failure, loss of gas supply, loss of water supply, fuel shortage, communication services failure and loss of drainage/waste removal.
Organised and/or deliberate disruption – Acts of terrorism and sabotage, act of war, arson, theft and labour disputes/industrial action
Environmental disasters – Tornado, hurricane, flood, snowstorm, drought, epidemics, earthquake, electrical storms, fire, subsidence, landslide, freezing conditions, contamination and environmental hazards

Organisations particularly at risk

Although, as mentioned previously, all sizes and types of organisation can be adversely impacted by an unplanned event, there are some that through the nature of their business or regulatory compliance are particularly at risk. These include:

- **Companies regulated by the FSA** – The FSA request companies to ensure that they can continue to function and meet regulatory obligations in the event of an unforeseen interruption.
- **Publicly listed companies** – Who need to implement the findings of the Turnbull report on internal risk management measures.
- **Local government and NHS Trusts** – The soon to be introduced Civil Contingencies bill imposes new duties on all councils to develop a proper structure to deal with emergency planning within their area.

Barriers to business continuity planning

To the uninitiated, business continuity planning can appear a costly and complex process that seems to have little or no immediate business benefit. This is because it is easier to do nothing and hope that an unplanned event does not happen.

The very nature of BCM involves the entire organisation at many levels and furthermore drives to the heart of the operation by asking uncomfortable questions about what is and is not important in a time of crisis. The need to understand all of the critical business processes that take place and how the breakdown of these will impact the organisation overall is vital, and will involve many different people at different levels, but without this there can be no plan.

It is important that the motives for BCM are clearly defined at the outset as this will help prevent confusion later in the project. These can range from being a public listed company who needs to implement the findings of the Turnbull report, through to a Governmental body that will gain a new area of responsibility with the Civil Contingencies bill

In many organisations this process will need to be undertaken voluntarily, but for some government regulation or industry requirements will drive the development of the plan. Either way it will be necessary to gain senior management support and sponsorship, else the entire process will fail.

Impact of a disaster

Although the immediate impact of an unplanned event will be apparent in lost revenue and the inability to deliver critical services, it is not these that cause so many organisations to ultimately fail.

It is the on-going impact that this interruption of business brings about that provides the ultimate "knock-out" blow for many organisations. These include:

- Loss of reputation and brand loyalty
- Customers may start to seek out alternative suppliers
- Supply chain partners will also look at alternatives
- Funding may disappear
- A need may be re-evaluated and deemed unnecessary

An organisation which fails to provide a minimum level of service to its customers following an unplanned event may not have a business to recover.

How to develop a business continuity plan

Who is responsible for BCM?

BCM has grown out of the need to provide IT disaster recovery. While this has focussed on IT systems and networks, BCM is broader in its scope and encompasses crisis management combined with business, as well as IT resumption. Drilling down from this top-level it will involve identifying key business functions and revenue sources as well as the need to maintain the reputation of the organisation as whole.

Together, these factors make BCM the shared responsibility of an organisation's entire senior management, from the chief executive through to the line-of business managers who are responsible for crucial business processes. Although IT remains central to the business continuity process, IT management alone cannot determine which processes are critical to the business and how much the company should pay to protect those resources.

It is important that BCM has the full support of an organisation's most senior committee to ensure the initiative does not stall. One member of this committee should be made the overall sponsor with responsibility for initiating BCM across the entire organisation. With this top level support it should be possible for the undoubted difficulties that will be faced in putting together the plan to be overcome.

An overall BCM co-ordinator should then be appointed to report directly to the senior committee member responsible for BCM. This person is ideally someone who understands the business structures and people. They require good programme management, communication and interpersonal skills and need to be a good team leader. In addition a budget must be allocated for the initial stages of the process.

For larger organisations matrix team management is the best method to approach BCM. The team will be drawn from existing managers within key divisions and or locations. It is expected that they will not be full time members of the team but will need to dedicate appropriate time to the BCM process.

BCM Principles

The Business Continuity Institute recommends that the following principles are utilised when devising and implementing a BCM plan:

- BCM is an integral part of corporate governance
- BCM activities must match, focus upon and directly support the business strategy and goals of the organisation
- BCM must provide organisational resilience to optimise product and service availability
- BCM must optimise cost efficiencies
- BCM is a business management process that is undertaken because it adds value rather than because of governance or regulatory considerations
- All BCM strategies, plans and solutions must be business owned and driven

Bearing these in mind it becomes easier to develop your BCM plan.

Overview of the BCM life-cycle

There are five steps that should be followed when developing a BCM plan:

1. Analyse your business
2. Assess the risks
3. Develop your strategy
4. Develop your plan
5. Rehearse the plan

Due to the rapidly changing nature of business conditions the process is not static, but cyclical. Once you have worked through and completed step 5 it is necessary to go back to step 1 and review the whole process again to ensure that any external or internal changes have not made elements of the plan redundant.

Analyse your business

This is the first stage of the BCM life-cycle as it is necessary to understand at the outset exactly where your business is vulnerable. You will need the fullest possible understanding of the important processes inside your organisation and between you and your customers and suppliers.

This stage of the process will also help to gain the involvement and understanding of other people and departments and will also help identify if any parts of the organisation already have plans or procedures in-place to deal with an unplanned event.

Assess the risks

There are two aspects to every risk to your organisation:

1. How likely is the risk to happen?
2. What effect will it have on your organisation?

BCM will provide a framework for assessing the impact of each one. Many organisations usually define their assessment in terms of cost. For example:

- 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.

1. Ask 'what if?' questions.
2. Ask what the worst-case scenario is.
3. Ask what functions and people are essential, and when.

Develop your strategy

Whatever type of organisation you are, you will probably choose one of the following strategies:

- Accept the risks – change nothing.
- Accept the risks, but make a mutual arrangement with another business or a business continuity partner to ensure that you have help after an incident.
- 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.

Your attitude to risk will be partly based on the costs of delivering effective business continuity. When working these out, remember to include both money and people's time.

Develop your plan

Once your strategy has been decided upon, the plan can be put in place. BCM plans will look different for different organisations. However, most good continuity plans share some important features:

- 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'.

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.

Rehearse your plan

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

Rehearsals are also good ways to train staff that have business continuity responsibilities. Possible ways to rehearse the plan include: paper-based exercises, telephone cascading and a full rehearsal.

You need to develop strategies that enable you to check the full plan with the minimum of cost and disruption.

BCM solutions

Types of solution

There are a number of different solutions available today designed to help an organisation both in the development and execution of their BCM plan. These include:

Business continuity planning

Here, help is provided to assist organisations to develop a workable business continuity plan. This includes help with:

- Preparing and presenting environmental analysis and business continuity plans
- Providing on-going management of business continuity projects and strategies

Business recovery solutions

A range of solutions that enable organisations to identify the best possible means of ensuring effective recovery following an unplanned event. These include:

- Mobile units that include the necessary systems and work area shipped to site
- On-line recovery
- Workplace recovery at a dedicated centre nearby

Managed continuity services

A partner will deliver and manage solutions in areas where the organisation may lack resource and expertise internally. Typically consisting of:

- Recovery rehearsal management – mutually agreed rehearsals to ensure that your business continuity plan is effective
- Continuity contract management – the partner takes on the responsibility for the relationships and service agreements that are already in place
- Data management – secure management and storage of data in real-time, without disruption to business operations
- Telecoms management – covering all call centre and general telecoms equipment

In-house or external

Due to cost considerations many organisations will utilise internal resources to develop and execute their BCM plan. While this may be realistic for a smaller organisation, a larger will typically require some external assistance.

To provide business continuity for critical business processes organisations who decide to facilitate it in-house must:

- Acquire, train and retain skilled personnel who can develop and manage the complex interdependencies and specialised elements of creating and maintaining a BCM plan
- Establish and maintain relationships with vendors to assure the quick delivery of replacement PCs, network hardware, desks, chairs, telephones, etc., in the event of a major incident
- Secure adequate funding from end-user departments to implement and maintain adequate business continuity protection
- Make adequate provisions for adding recovery support staff in the event of a regional or natural disaster.
- Ensure that sufficient latent capacity will be immediately available to assure rapid failover and recovery
- Test the capacity availability without disrupting ongoing operations
- House failover equipment in a separate location from the main production equipment and provide further redundancies, such as obtaining electrical supplies from different sources

Using a BCM partner for some or all of these requirements can be attractive for organisations that prefer to focus already scarce resources on day-to-day operational issues. By establishing a long-term strategic relationship with a reputable BCM partner organisations can gain a competitive advantage.

Engaging a BCM partner enables these organisations to:

- Leverage the partner's extensive investments in the latest technology, continuous improvements to methodologies, and skilled people
- Benefit from the expertise gained in solving problems for a variety of organisations with similar requirements
- Use the partner's backup facilities and resources
- Take advantage of the partner's economies of scale on assets, resources and procurement to help enable a lower cost of operation and significantly less risk
- Concentrate on achieving core business growth objectives.

Ten things to look for in a BCM partner

BCM is critical to your business and although there are now an increasing number of organisations offering BCM services and solutions, the partner you choose must deliver support that addresses your company's critical business processes.

Below are some of the factors to utilise when evaluating a potential BCM partner:

1. A focus on business continuity, separate from traditional disaster recovery services
2. Integrated solutions to assure availability of non-data centre resources, including networks, end-user workspace and call centres
3. Experience across a wide range of industries and disaster scenarios
4. Sufficient resources to accommodate multiple recovery clients in the event of a widespread disaster
5. The ability to understand the integration of IT with business strategy, and define the risks and impacts of a disruption to critical IT infrastructures
6. An understanding of e-commerce dependencies and business-critical requirements
7. Skills and resources to manage complex business continuity programs in a rapidly changing, networked IT environment
8. A significant investment in modern BCM facilities
9. Support for multi-vendor and multi-platform IT environments
10. A proven track record in recovery and technical support

Conclusion

BCM is not just about reacting to an incident. It's not just about disaster recovery, crisis management, risk management control or technology recovery. And it's not just a professional specialist discipline. BCM is a business owned and driven activity that can provide the strategic and operational framework to review the way your organisation provides its products and services and increase its resilience to disruption, interruption or loss.

While larger organisations generally have more to lose and more ways to lose it than smaller organisations, smaller firms often suffer the most devastating results from seemingly minor business interruptions. Small size imposes stricter limits on the ability of an organisation to absorb losses and respond to interruptions.

The key to recovery is time. Following an unplanned event, the organisation which recovers in the shortest possible time will mitigate their losses to an optimum level.

That is why BCM is important for organisations of all sizes. It should be viewed as a cornerstone to good corporate practice, embracing risk, security, insurance, legal, operational and safety issues.

ICM resources and investment

ICM is a specialist provider of consultancy and solutions for all aspects of business continuity. We provide completely flexible support from local service and recovery centres, strategically located throughout the UK.

Our resources include:

- **Risk Analysis** – first stage when producing a Business Continuity Plan
- **Plan Development** – helping clients identify potential strategies suitable to the recommendations from the Risk Analysis
- **Security Management** – assistance in achieving compliance with legislation i.e. DPA and BS7799 and review existing security controls and procedures
- **Project Management** – support from our highly skilled team of consultants and technical support personnel, allowing staff to focus on primary business objectives

- **Relocatable Recovery** – ship-to-site replacement system installed and linked to the existing infrastructure
- **Mobile Recovery** – a replacement data centre, complete with required IT systems and experienced engineers directly to a pre-designated site
- **Online Recovery** – hosting of critical duplicate systems with immediate failover to on-line data, 24x7
- **Workplace Recovery** – Replica working environment consisting of desktop PCs or workstations, servers and central IT services and programmable telephony designed to match office and call centre requirements. ICM have a total of 3000 workplace positions situated at 10 workplace centres in strategically chosen areas throughout the UK

- **Recovery Net –** a platform name for a family of network based recovery solutions through the ICM Group ATM Cellstream at each of our centres.
  Solutions include:-
      - Connect – Wide Area Connectivity
      - Internet – Internet Service Provision
      - Email Recovery Solutions
- **Multi Vendor –** Provisions for multi vendor hardware platforms from servers to mainframes such as Compaq Intel servers, Compaq Alpha, Compaq VAX, IBM AS400 and I series, IBM RS6000 p-series, Sun Enterprise and Sunfire systems, HP-UX systems
- **Telecoms Solutions –** Provisions for Nortel Meridian Option 11 and Option 81 Digital Switches with Call Centre capability complete with Digital Handsets and headset availability. In addition, Wallboard capability and ATM network information is available in each ICM centre

ICM case studies

Building society

A major building society decided to implement a more comprehensive business continuity strategy with the aim of ensuring that in the event of a disaster occurring, the interests of all stakeholders in the business would be protected.

The Society had previously provided for office recovery by utilising their own alternative premises, close to their head office. However, growth in the Society's business over recent years meant that these arrangements were no longer viable. They therefore decided to partner with a business continuity specialist that could provide a cost effective solution within a short timeframe.

They required an alternative facility that was close to their head office, able to support their IT systems and offer the voice and data communications capability they required.

ICM had a recovery centre within six miles of the organisation's head office with communication facilities matching their requirements. This combined with technical skills and resources fulfilled the society's requirements.

The Society subscribed to ICM for an occupancy of the recovery centre for 150 of their staff in the event of loss of access to their site. The solution ICM provides includes access to a high specification desktop PC for each of the 150 positions, 120 analogue telephones and 30 digital telephones with ACD capability together with other much needed requirements.

The solution provides the Society with a replica of their own head office environment, enabling them to continue business with minimal disruption, whatever the circumstances. The close proximity of ICM's business recovery centre also enables the Society to utilise the premises for system and invocation testing.

Health Authority

A Health authority had been a customer of ICM since 1995, purchasing equipment on an ad-hoc basis. As the relationship developed over the years, the Authority began to look to ICM for increasingly comprehensive support and more recently, for disaster recovery services.

Having been under increasing pressure from the NHS to institute a business continuity plan, the Authority now works closely with ICM to ensure that their systems are safeguarded for every eventuality.

As a specialist provider of business continuity solutions, ICM has been able to offer a high level of consultancy, helping to limit the potential causes and impact of any event which may threaten the ongoing continuity of the organisation's key processes.

ICM was also on hand when the Authority was a victim of a burglary in which all their PCs were stolen, shipping replacement systems to site, so that everything was back up and running as normal within 24 hours.

This document should be read as a guide only and is not intended to be legally binding.

For more information, visit www.icmore.co.uk