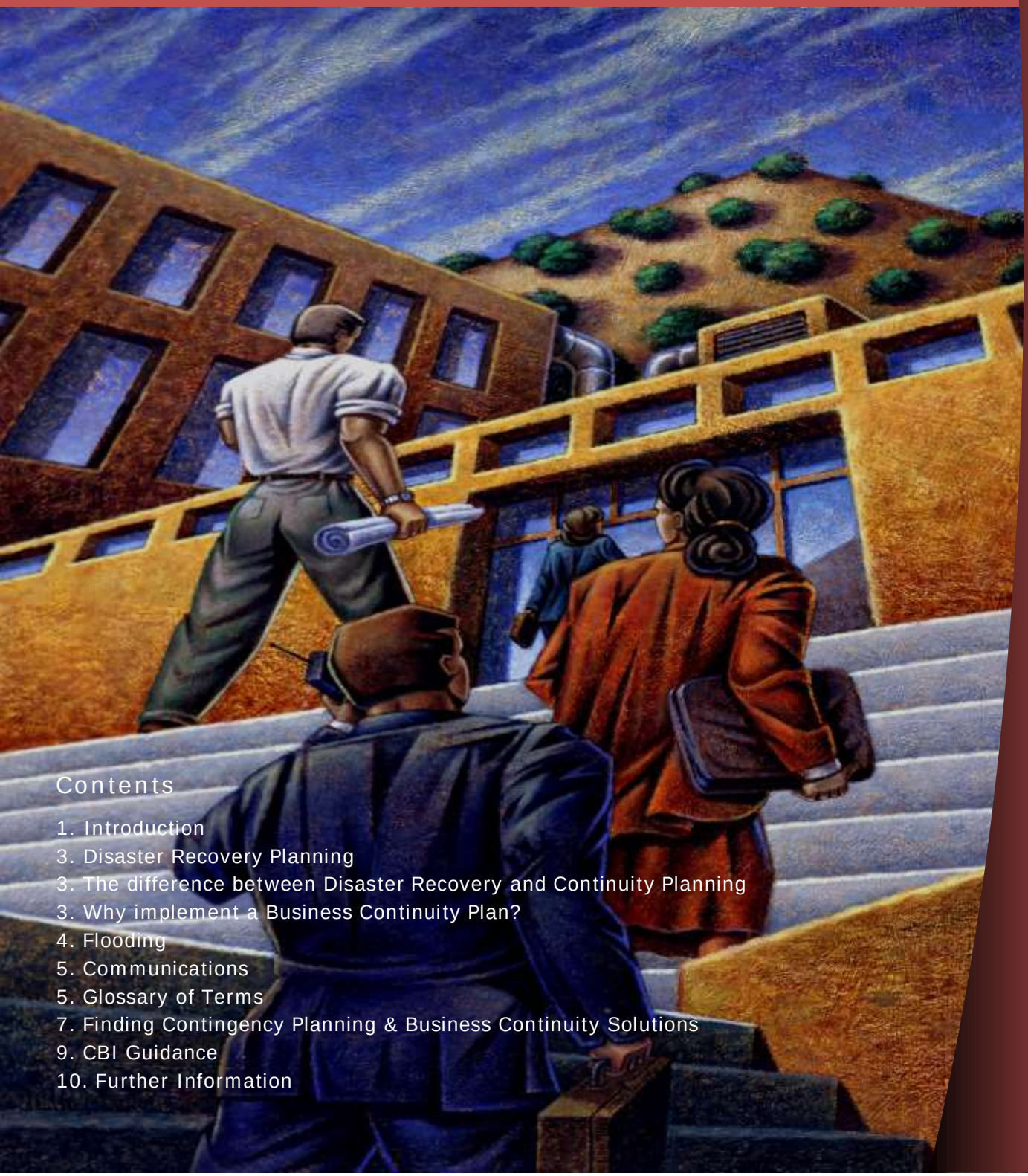
Business Continuity Planning

… the livelihood of your business depends on it

Expert knowledge means success



Contents

1. Introduction
3. Disaster Recovery Planning
3. The difference between Disaster Recovery and Continuity Planning
3. Why implement a Business Continuity Plan?
4. Flooding
5. Communications
5. Glossary of Terms
7. Finding Contingency Planning & Business Continuity Solutions
9. CBI Guidance
10. Further Information

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

Introduction

Business continuity management is an ongoing process of risk assessment and management with the purpose of ensuring that the business can continue if risks materialise. These risks could be from the external environment (over which you have no control, such as power failure) or from within your organisation, such as deliberate or accidental damage to systems. Business continuity is not just concerned with disaster recovery; it addresses anything that could affect the continuity of service over the long term, such as staff shortages in specialist areas.

In the UK, we have become accustomed to the threats of fires, floods and bombs affecting how we live and work. Every organisation needs to look at its own vulnerabilities and dependencies and to take actions that will minimise the impact of potentially disruptive incidents and to implement a Business Continuity capability. And it's not just major tragic incidents that can severely disrupt your business:

- a fire in an adjacent building could deny you access to your premises for several days or more;
- a leaking vending machine on the floor above could flood your office and render it unusable for weeks;
- theft of your computer equipment could prevent you accessing computer-held data for days, you could even lose this data permanently.

By their very nature, disasters are not generally planned – they just happen - and their cause is often totally beyond your control. The Tsunami on Boxing Day 2004 and more recently the 2011 earthquake in Japan affected the lives and businesses of millions of people. Some planned disasters may be beyond our foresight: who would have imagined that two jet aircraft would be flown into two of the world's most famous skyscrapers? The basic concept of business continuity is to "plan for *when* not *if*", and a business continuity plan will enable your business to cope with the traumas and disruptions should they occur.

Power cuts, industrial action and transport failures show the fragility of UK businesses in the face of unforeseen events. Computer viruses have caused havoc for thousands of businesses across the UK.

Typical Disaster Phases

1. CRISIS
This happens within the first few hours after the incident starts – for example, caused by damage to premises or restricted access to buildings etc.

2. EMERGENCY RESPONSE
This may last for a few minutes or a few hours after the crisis phase. During this time, the situation has to be assessed and decisions made quickly as to rapid recovery etc.

3. RECOVERY
This may last several months following the disaster. It ends when normal operation can restart. During this phase, essential or primary operations will restart and continue in *recovery format.*

4. RESTORATION
Conditions are restored to normal. Planning for this phase might start within a few days of the actual incident. If there was physical damage to the premises, this phase will be delayed.

Source: BIS

Has 7/7 made your business rethink its Continuity Plan?

A research report commissioned by AXA concluded that UK's small businesses are still failing to make adequate provision for business interruptions.

Of the SMEs questioned after the 7 July terrorist attacks:

- 75% had not reviewed their business approaches;
- 46% didn't have a business continuity plan; and
- 37% of senior managers admitted they relied on luck when making an important business decision.

These findings are of particular concern if representative of SMEs in general, given that SMEs account for over 99% of the total number of UK firms, generate 52% of total revenue and employ 56% of the private sector.

Top 10 disclosed* data losses in 2005**

Rank	Company	How lost	No. of customers affected
1	Card Systems	Hacking	40,000,000
2	CitiFinancial	Lost backup tape	3,900,000
3	DSW/Retail Ventures	Hacking	1,300,000
4	Bank of America	Lost backup tape	1,200,000
5	Wachovia, Bank of America, PNC Financial Services,Commerce Bancorp	Dishonest insiders	676,000
6	Time Warner	Lost backup tape	600,000
7	LexisNexis	Passwords	280,000
8	University of S.California	Hacking	270,000
9	Ameritrade	Lost backup tape	200,000
10	San Jose Medical Group	Stolen Computer	185,000

Source: DISUK

*In parts of the US, it is obligatory to disclose data losses. In the UK there is no such obligation.
**Note. This information was compiled prior to the Buncefield Oil Depot disaster on 11 Dec 2005

Worryingly, one in four companies which experiences a disaster never recovers. Despite this, when surveyed, fewer than 50% of organisations in the UK admitted to having a back-up plan in place for when things go wrong, leaving them ill-equipped to survive the most common disasters. In response to this, AXA[1] has launched two free guides to help SMEs take control of their future by helping them to prepare for the worst.

Normal operations of most businesses are dependent on a number of basic facilities being in place and operational. A small disruption can have a big impact on your business, so imagine the impact that a major incident could have. The immediate and physical damage of a fire in your normal work-place is probably obvious, but have you considered the wider impact of such an incident - being unable to communicate with customers and suppliers for several days, being unable to progress current work, losing paper-based information, losing your computer services, and could you return to normal once the dust and smoke has settled.

Business continuity planning enables you to determine the risks that you may be exposed to, identify and quantify the impact to your business of disruptive events and implement appropriate contingency arrangements to ensure your business survival.

Entitled *Business 4 Tomorrow*, the AXA guide sets out for the first time a business continuity planning process designed specifically for small businesses. The process, developed by AXA's risk specialists, helps make business continuity planning more time and cost efficient by focusing on key risk areas one at a time. This ensures that high-risk areas of the business can be thoroughly assessed and secured, which makes it easier to pull together a comprehensive, overarching continuity plan based on a simple 'crisis response template'. It is staggering that fewer than 50% of SMEs have not taken the simple, yet necessary steps to protect the future of their business. If they do this, not only will it give them peace of mind, but it will also help them manage their insurance premiums. Disaster can strike at any time, but businesses don't need to be unprepared. By thinking and preparing for potential threats to their business, managers can take pro-active steps to protect themselves against the majority of disasters.

AXA's second guide entitled "*Business Continuity Guide for Small Businesses*" provides a step by step guide to business continuity planning and includes case studies and a sample plan to help get you started. Its message is that business continuity needn't be complicated and doesn't have to cover every eventuality or every business process, just those that are most critical.

Financial Service providers must strengthen Business Continuity plans

A study of the UK financial services industry's ability to cope with major operational disruptions has determined that the industry would benefit from stronger business continuity plans that focussed more heavily on IT.

The study asked:

- How resilient is the UK financial sector?
- How quickly could the sector recover from major operational disruption?
- Do firms plan and prepare effectively?
- Are there any concentrations or dependencies that could be potential areas of vulnerability?
- What action is needed to improve the resilience or recovery capability of the sector?

The study, named The Resilience Benchmarking Project, and published on 14 December 2005 was led by the Financial Services Community (the FSC is a tripartite comprising the HM Treasury, the Financial Services Authority and the Bank of England). It surveyed the disaster recovery processes of more than 60 of the UK's financial services companies.

It concluded that:

- The industry had 'highly resilient' IT systems that could recover quickly.
- Most companies could recover 60% to 80% of their normal operations within 4 hours, and 80% to 100% by the next day.
- There was a heavy concentration of back-up sites within London – a particular point of concern.
- 28% of companies had no policy of testing their outsourcing suppliers' disaster recovery capabilities.
- 20% of companies had not tested critical backup tapes in the past six months.
- 13% of companies had not tested mirrored IT systems with the primary system turned off.

The survey also determined that the cost of suspending or curtailing operations for businesses in this sector was between £500,000 and £25m depending on the operation. Not surprisingly, faced with this information, "almost all participant firms have already indicated that they are planning to make changes to their business continuity arrangements".

Source: FSC

Further information on the Resilience Benchmarking Project, is available on the FSC web site: www.fsc.gov.uk

"Businesses are operating in a world full of risk and uncertainty yet identifying and managing risk is still often poorly understood. Most companies will survive if they ensure risk management is central to their business ethos and updated in line

regularly with their business plan and mission." The AXA guide aims to demystify risk analysis by providing clear responses to frequently asked questions about business continuity, an easy to follow guide to business continuity planning and sample paperwork that can be used as the basis for a small business continuity plan.

Facilities	Considerations
Work-place	• use another branch of your company • use temporary facilities from a specialist supplier • work from home
Staffing	• identify core skills and source of temporary resources with these skills • cross-train staff on critical activities
Computer and telephony services recovery	• identify critical services and the technology required to support these services • arrange for fast-track delivery, installation and rebuild of your critical services • build resilience into your IT and communications infrastructures to prevent any single point failures • redirect your data feeds, voice, fax etc
Data and information restoration	• ensure all critical data is protected, copied, backed up, held safe • ensure all critical data can be accessed after loss of the master copy • ensure all critical data can be restored from backups • ensure that your business understands and accepts that some data may be irretrievably lost

Disaster Recovery Planning

Disaster Recovery Planning is an important component of your overall business continuity plan and will ensure that you have the required recovery facilities and procedures to provide alternatives if key components are lost, for example, if some or all of the important facilities could not be recovered, your ability to resume normal business operations could be severely compromised or prevented.

A business continuity plan can help a small business to overcome potentially catastrophic disasters by putting in place back up systems and processes to keep the business going both during and after a calamity.

Preparation is key to the success and longevity of any small business while a lack of contingency planning can be devastating:

- 90% of businesses that lose data from a disaster are forced to shut within two years;
- 80% of businesses without a well-structured recovery plan are forced to shut within 12 months of flood or fire;
- 43% of companies that experience a disaster never recover;
- Companies experiencing a computer outage lasting longer than ten days will never recover their full financial capacity;
- Fewer than 50% of all organisations in the UK have a business continuity plan.

The difference between Disaster Recovery and Continuity Planning

A disaster recovery plan is reactive and usually focuses on recovering the computing environment. Although work may be done to harden the computing infrastructure to prevent a disaster, the plan's main purpose is to recover from damage to the infrastructure. In contrast, a business continuity or contingency plan is not only proactive, but it is also targeted at keeping the business running during an event, not just recovering the computers after the fact. As part of its continuity planning process, a company needs to review the continuity or recovery of manufacturing, packaging, warehousing, shipping, customer support, and any other facilities or operations that are critical to the company's survival.

Source: HP - ensuring survival: developing a business continuity plan strategy brief

Why implement a Business Continuity Plan?

Your business operations are almost certainly dependent on a number of key facilities:

- your normal place of work
- your staff
- your computer services
- your telephone services
- your data and information

"One of the problems is that sensitive information can be protected on a securely encrypted computer with as many algorithms as there are grains of sand on a beach, but all it needs is for one person to jot down a note at 5pm when they are feeling weary, have the note couriered to a third party and put the firm's whole security at risk."

Dr Phil Kelly, Liverpool John Moores University

- your business processes and procedures.

Imagine losing some or all of these facilities, or being denied access to them for a prolonged period of time; what would be the impact to you and your business:

- Could you contact suppliers and clients?
- Could suppliers and clients contact you?
- Could you pay suppliers?
- Could you receive payments from clients and chase for late payments?
- Could you continue to provide services and products to your clients?
- Could you retain the confidence of your clients to deliver, or would they take their custom elsewhere?
- Would you lose your market share?
- Would your business name and reputation be damaged?

Source: www.prubusiness.co.uk

Flooding

Climate change experts predict an increase in extreme weather events and it is likely that severe floods will be a regular occurrence and something that the UK will have to learn to live with. The Environment Agency estimates that the average cost of flooding in England is £1.15 billion, of which £401 billion is to business, including damage to both tangible items such as premises and equipment and less tangible items such as market share.

In August 2007, Sir Michael Pitt was asked by the Government to carry out a review of the flood-related emergencies that occurred during the summer of 2007.

The interim report was published in December 2007 with the following objectives:

- To identify issues that require urgent action.
- To set the direction for the remainder of the Review.
- To provide a document for consultation before the final report is published in summer 2008.

On 17 December 2007, the Secretary of State for the Environment, on behalf of the Government, accepted the urgent recommendations in the interim report, and pledged to work with all relevant organisations to implement them. These recommendations include improving an understanding of surface water flooding and areas most at risk from it. Surface water flooding (caused by sudden heavy rainfall, which cannot drain away adequately) was one of the main contributions to the 2007 flooding.

The interim report identifies a significant number of other findings, many of which are likely to be acted on in the coming months. These include a requirement for PPS 25 to be applied rigorously to ensure that the risk of flooding, from all sources, is adequately considered before planning permission is given for development. It also includes restrictions on permitted development that allow land to be covered with impermeable surfaces (such as patios, driveways and garden sheds) that contribute to the problems caused by surface water.

In addition, the European Commission has published a new directive (The Floods Directive 2007/60/EC) on the assessment and management of flood risks. It aims to reduce the consequences to human health, the environment, cultural heritage and economic activity caused by floods. Member states are required to carry out preliminary flood risk assessments, prepare flood hazard and risk maps, and produce flood risk management plans.

The Floods Directive came into force in November 2007 and member states have until 26 November 2009 to transpose it into national law. The Floods Directive applies to all types of floods such as rivers, flash floods, urban floods and coastal floods. Its purpose is to establish a framework for the assessment and management of flood risks. It aims to reduce the consequences to human health, the environment, cultural heritage and economic activity caused by floods. The Government is planning to publish a consultation on the draft legislation in February 2009 in readiness for the legislation coming into force later in 2009.

The extent of flood damage and the extent to which action is taken to prevent flood damage will affect the approach taken by insurance companies to insuring properties in high flood-risk areas. There is currently a willingness to carry on insuring certain categories of residential and small business property but this may change and much depends on the Government's approach to flood defence work.

Examples of risks to your business

Strategic risks:
Increased competition

Financial risks:
Financial operations, cash flow, credit extension, debt recovery, foreign exchange, interest rates

Operational risks:
Breakdown or theft of equipment, supplier reliance

IT risks:
Data security and protection

Compliance risks:
Compliance with industry and business laws and regulations

Health & safety risks:
Assessment and management of health and safety risks

Source: Business Link

For these reasons, managing flood risk will be an important issue over the next few years, the issue being made particularly pressing because of the additional three million new homes promised by the Government by 2020 to address the chronic housing shortage. It is essential that these new properties are not built in areas that are at a high risk of flooding and that they do not exacerbate the existing flood risk either through the additional demands on drainage or by the additional coverage of land with impermeable surfaces preventing the proper drainage of surface water.

Communications

Whilst the UK Public Switched Telephony Network is a reliable infrastructure (quoting 99.999% availability) the telephone circuits installed by carriers that connect to it and the connection to your business premises may be less reliable. It may be subject to power cuts, building work damage, terrorism, viruses or other disruptions. The resilience of "The Last Mile" can be increased by installing a second circuit from either the same or an alternate exchange, although this can be expensive. Alternatively, a service can be provided at a carrier's exchange that both re-routes inbound phone calls to alternative locations and records all inbound and outbound calls.

Any business continuity plan should consider how loss of normal communications could be replaced by call re-routing, SMS, e-mail, voicemail and paging as appropriate to your business. One thing that should not be forgotten is that your customers and employees need to be kept aware that you are still in business and how they can contact you.

Glossary of Terms

Business Continuity Management:
Management disciplines, processes and techniques which seek to provide the means for continuous operation of essential business functions under every circumstance.

Business Continuity Planning:
Advance planning and preparations which are essential to identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan[s] which ensure continuity of organisational services in the event of an emergency or disaster.

Business Continuity Programme:
An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans and ensure continuity of services.

Business Impact Analysis [BIA]:
Measures the effect of resource loss and escalating losses over time.

Contingency Plan:
A plan of action to be followed in the event of a disaster or an emergency occurring which threatens to disrupt the continuity of normal business activities. This also seeks to restore operational capabilities.

Crisis:
An abnormal situation, or perception which threatens the operations, staff, customers or reputation of an enterprise.

Crisis Plan:
A plan of action designed to support the crisis management team when dealing with a specific emergency situation which might threaten operations, staff, customers or reputation of an enterprise.

Declaration [of disaster]:
A formal statement that a state of disaster has occurred.

Disaster:
Any accidental, natural or malicious event which threatens or disrupts normal operations, or services.

Disaster Recovery Plan [DRP]: A plan to resume, or recover, a specific essential operation, function or process of an enterprise.

Disaster Recovery:
The process of returning a business function to a state of normal operations at an interim minimal survival level and/or re-establishing full scale operations.

It makes sense...

A viable business continuity strategy will ensure that:

- Your mission-critical systems are safeguarded;
- Your optimum service levels are maintained;
- The impact of a disaster on your business is minimised.

"80% of businesses affected by a major incident either never re-open or close within 18 months."

Source: AXA

Emergency:
An actual or impending situation that may cause injury, loss of life, disruption of property or interfere with business operations to such an extent to pose a threat of disaster.

Emergency Plan:
A plan which supports the emergency management team by providing them with information and guidelines.

Enterprise:
An organisation, a corporate entity; a firm, an establishment, a public or government body, department or agency; a business charity.

Financial Impact:
An operating expense that continues following an interruption or disaster which as a result, cannot be offset by income and directly affects the financial position of the enterprise.

Impact:
The cost to the enterprise - could be measured in financial terms.

Incident:
Any event that may be or may lead to a disaster.

Invocation:
A formal notification to a service provider that its services are required.

Operational Impact:
An impact that is not quantifiable in financial terms, but its effects may be among the most severe in determining the survival of an enterprise following a disaster.

Outage:
The interruption of automated processing systems, support services or essential business operations which may result in the enterprise's inability to provide service for some time.

Period of tolerance:
The period of time in which an incident can escalate to a potential disaster.

Recovery Plan:
A plan to resume a specific essential operation, function or process of an enterprise. Traditionally referred to as a Disaster Recovery Plan.

Recovery Strategy:
A pre-defined, pre-tested management approved course of action to be employed in response to a business disruption, interruption or disaster.

Recovery Team:
A group of individuals given responsibility for the co-ordination and response to an emergency or recovering a process or function in the event of a disaster.

Resilience:
The ability of a system or process to absorb the impact of component failure and continue to provide an acceptable level of service.

Response:
The reaction to an incident or emergency in order to assess the level of containment and control activity required.

Restoration:
The process of planning for and implementing full-scale business operations which allow the organisation to return to a normal service level.

Resumption:
The process of planning for and/or implementing the recovery of critical business operations immediately following an interruption or disaster.

Risk Reduction or Mitigation:
The implementation of the preventative measures which risk assessment has identified.

Service Level Agreement [SLA]:
An agreement between a service provider and service user as to the nature, quality, availability and scope of the service to be provided.

Site Access Denial:
Any disturbance or activity within the area surrounding the site which renders the site unavailable e.g. fire, flood, riot, strike.

Structured Walk-Through:
An exercise in which team members verbally review each step of a plan to assess its effectiveness, identify enhancements, constraints and deficiencies.

System Denial:
A failure of a computerised system for a protracted period, which may impact an enterprise's ability to sustain its normal business activities.

System Recovery:
The procedures for rebuilding a computerised system to the condition where it is ready to accept data and applications.

System Restore:
The procedures necessary to get a system into an operable condition where it is possible to run the application software against the available data.

Source: BT CommSure
www.btcommsure.com

"Evidence shows that every five years, 20% of companies will suffer a major disruption through fire, flood or storm, power failures, terrorism and hardware/software failures.

Of those companies which do not have Business Continuity plans, 80% fail within 13 months of such an incident. Those who successfully restore their business have seen the company value rise."

John Sharp, CEO, The Business Continuity Institute.

Finding Contingency Planning & Business Continuity Solutions

Business Continuity World

Business continuity and contingency planning are of course essential and unavoidable tasks. However, the creation of a sound business continuity and contingency plan is a complex undertaking, involving a number of stages and discrete activities. For example, initially it is necessary to understand the underlying risks and the potential impacts of disaster.... these are the building blocks upon which a sensible business continuity plan or disaster recovery plan should be built. Then the plan itself must be created... which of course is far from trivial. Then there are the maintenance and testing phases, to ensure that the plan remains current. *Contingency Planning & Business Continuity World* is designed to consider all these stages and to catalogue some of the most highly acclaimed support products. Here you will find software to assist with business impact analysis and risk analysis. You will also find links to products to help you create and maintain the plan itself, as well as audit the plan and the arrangements in place to support it.
www.business-continuity-world.com

Business Continuity Institute

The Business Continuity Institute was established to provide opportunities to obtain guidance and support for business continuity professionals. The Business Continuity Institute provides an internationally recognised status and its wider role is to promote the highest standards of professional competence and commercial ethics in the provision and maintenance of business continuity management services. This web site contains a wealth of information and resources for both the business continuity novice and expert as well as allowing members the opportunity to communicate and network with each other.
www.thebci.org

IBM

Business continuity is vital to business success. It can no longer remain the concern of the IT department alone. How do you determine the continuity and recovery requirements of your business? How do you identify and integrate critical business and IT priorities into a comprehensive continuity programme? Where do you start?
www-01.ibm.com/software/uk/itsolutions/managing-business-infrastructure/business-continuity-and-recovery/

GlobalContinuity.Com

GlobalContinuity.com is the world's most comprehensive resource for business continuity and disaster recovery information. Whether you are new to these subjects or a seasoned professional you will find news and articles relevant to your needs in this extensive portal.
www.globalcontinuity.com

Survive

Launched in 1989, Survive has grown throughout the world to become the leading forum for expertise and information exchange among business continuity management practitioners and professionals, and all managers and directors with responsibility for ensuring the resilience and ultimate survival of their companies.
www.survive.com

Continuity Central

Continuity Central provides a constantly updated one-stop resource of business continuity information. Expert or novice, this site will meet your needs, keeping you up-to-date with all that happens in this fast changing market and enabling you to rapidly and comprehensively research the subject.
www.continuitycentral.com

SunGard

It's not just about protecting data. It's about keeping people connected to it so your business runs uninterrupted – 365 days a year. By combining technology, redundant infrastructure and technical expertise SunGard helps ensure your organisation's continuous access to its mission critical information. From the zero downtime required by e-commerce to the traditional disaster recovery requirements of 24 – 48 hours, SunGard can meet your needs.
www.availability.sungard.com

"Rothstein Catalogue" on Disaster Recovery

An excellent source for hundreds of books, software tools, videos & research reports.
www.disasterrecoverybooks.com/

"Preventing chaos in a crisis is more efficient than having to recover from a disaster. Where catastrophes have previously occurred as a result of failure to deal with an initial crisis, Business Continuity Management offers a solution. It is different from disaster recovery planning since it is proactive and concentrates on everything that is needed to continue the key business processes, whatever the catastrophe. A realistic understanding of good Risk Management is crucial, linked to the overall objective, which is a continuing process of which the document marked 'plan' is simply a written presentation to be adhered to in the event of a crisis."

Visor Consultants Limited
212 Piccadilly London W1V 9LD

Disaster Recovery World

It is now generally recognised that business continuity planning and disaster recovery planning are vital activities. However, the creation of (and maintenance of) a sound business continuity and disaster recovery plan, is a complex undertaking, involving a series of steps. Prior to creation of the plan itself, it is essential to consider the potential impacts of disaster and to understand the underlying risks: these are the foundations upon which a sound business continuity plan or disaster recovery plan should be built.

Following these activities the plan itself must be constructed - no small task. This itself must then be maintained, tested and audited to ensure that it remains appropriate to the needs of the organisation.

And what about the support infrastructure and services? Business Continuity Planning & Disaster Recovery World is designed to consider all these issues and to catalogue some of the most highly acclaimed products and services. Here you will find software to assist with BIA and risk analysis, as well as links to tools/services to help you create, maintain and audit the plan itself. Whether you are entirely new to business continuity and disaster recovery planning, or whether you already have a proven and established plan, the directory should be of real value.
www.disasterrecoveryworld.com

The Business Continuity Directory

Business continuity planning and disaster recovery planning are fundamental to the well being of an organisation. Clearly, they are intended to ensure continuity in the face of unforeseen or difficult circumstances. Planning for these situations is not always straightforward of course, and neither is identifying suitable sources of information, services and products. The requisite planning tasks themselves can also be challenging.... none more so than the building of the plan itself.

The Directory offers guidance in many of these areas - through the provision of information and guidelines and via the identification of suitable tools and suppliers.
www.business-continuity-and-disaster-recovery-world.co.uk

GemaTech

GemaTech are telecom business continuity specialists. They invest in and commercially develop leading edge tele-business products that solve today's key communications challenges. Their Business Continuity Manager software claims to deliver a credible disaster recovery solution for switches enabling 100% of the workforce to be fully operational minutes after disaster strikes.

Voice communications are sometimes overlooked in business continuity plans. Although web traffic and e-mails are fairly easy to redirect, voice telecoms are not as straightforward and are just as important. If your main switchboard is unavailable, orders and business are lost.

GemaTech provide a way of diverting individual calls that allow thousands of employees' numbers to be rerouted instantly to other individual numbers in the event of business disruption.
www.gematech.com

ICM Continuity Services

ICM Business Continuity Services has merged with NDR (Network Data Recovery). They provide a range of business continuity services and products from fully equipped business recovery centres to remote connection or data replication. With a client list of over 1400, including many Top UK 100 companies, and having achieved a 98.9% satisfaction rate in the latest customer survey, NDR is recognised as a leading supplier of multi-platform disaster recovery services in the UK.
www.icm-continuity.co.uk

Symbiant

Symbiant provide bespoke web based dynamic data management solutions and e-business software. Their multi-award winning software is used by some of the world's largest companies and leading financial organisations. Their main expertise is within the Internal Audit and Risk Management arena. Their products are web based, which makes them easy to deploy and reduces costs.
www.symbiant.co.uk

Businesses get disaster planning help

Local authorities are now obliged to help businesses plan for disasters such as fires, terrorist attacks and bird flu. A joint survey by the Cabinet Office and the Chartered Management Institute of 1,150 firms and public sector organisations found that while disaster planning was seen as important by the majority, less than half had actually put together a plan.

The new services, launched on 15 May 2006 under the Civil Contingencies Act, are designed to ensure that disasters cause as little damage to the economy as possible and businesses continue to trade. The Government believes that robust, flexible business continuity management (BCM) is fundamental to the preparedness of all organisations across the public, private and voluntary sectors and this is reflected by the duties on responders under the Civil Contingencies Act both in terms of responders' internal BCM, and the duty on Local Authorities to promote BCM to commercial and voluntary organisations in their area. For more information contact your local authority.

Steelhenge

Steelhenge is focused on preparing clients to respond effectively to incidents, crises, emergencies or disasters that cause disruption to their normal business. Their aim is to ensure recovery from any set back with maximum speed and minimum loss of assets, reputation or momentum.
www.steelhenge.co.uk

Beeches Consulting

Beeches Consulting are independent consultants in Business Continuity and IT Disaster Recovery planning.
www.beechesconsulting.com

Callagenix

Callagenix specialise in Telephone Business Continuity and Disaster Recovery Services. They provide a wide variety of business telecommunications phone services from simple number redirects through to comprehensive virtual switchboard services. Like buildings blocks, you can take as many services as you like and fit them together to provide an integrated service.
www.callagenix.com/dr

CBI Guidance

The CBI worked with security and defence specialists QinetiQ and drew on MI5 advice to produce a downloadable document containing some new tips on continuity and security planning that covers the following six main areas:

- Business Survival: The Critical factors
  - It is critical that continuity plans are regularly reviewed and tested.
  - All staff should be trained to execute your plans.
  - Consider your position in the immediate aftermath of an event.
  - Do you have a separate location to go to, to continue operations?
- Protecting Intellectual Property
  - How dependent are you on your network?
  - Do you have an incident management programme to manage the response to IT security incidents?
  - What to consider.
- Validation of Staff
  - Do you really know who works for you?
  - Where IT services are outsourced, do vet external suppliers.
  - Make sure you know who has left your company.
- Controlling Entries & Exits
  Physical Security: Technology
  - Incoming packages and mail can be a potential source of danger.
  - Remember fixed security systems can all be thwarted in time.
- Physical Security: Basics
  - Contact your Crime Reduction Officer or local Counter Terrorism Security Advisor.

SMEs – Take Note!

British Standard for Continuity BS 25999 series provides information on measures businesses should take to protect themselves in the event of disaster.

BS 25999 is a Business Continuity Management standard in two parts:

- The first, "BS 25999-1:2006 Business Continuity Management. Code of Practice", takes the form of general guidance and seeks to establish processes, principles and terminology for Business Continuity Management.
- The second, "BS 25999-2:2007 Specification for Business Continuity Management", specifies requirements for implementing, operating and improving a documented Business Continuity Management System (BCMS), describing only requirements that can be objectively and independently audited.

Certification (independent verification) to this standard is available from certification bodies accredited by the United Kingdom Accreditation Service (UKAS) and is a multi stage process usually involving a number assessment visits. The assessor will then make a recommendation that the organization receive certification or not. After initial certification a number of surveillance visits are made as per a plan to ensure that the organization is still in compliance.

For further information visit:
www.bsi-global.com

CBI on Business Continuity

"In a year that has seen mainland terrorism, a major incident at the UK's fifth largest oil and petrol distribution depot and natural disasters too numerous to mention across the globe, everyone in business needs to spend some time this January re-assessing their business risk.

In the immediate aftermath of any form of incident, continuity planning becomes something of a buzz word but it is increasingly clear that many firms still don't have the necessary plans in place.

Consider Buncefield: it was a miracle that no-one was killed, but more than anything it showed that the unexpected can happen at any time.

Having the right plan and the right people in the right places can ensure that your business survives no matter what.

It is a vital self-help insurance policy that everyone in business must have."

Sir Digby Jones,
(when CBI Director General)
2 January 2006

Further Information

This guide is for general interest - it is always essential to take advice on specific issues. We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

References:

[1] The AXA Business 4 Tomorrow guide and the Business Continuity Guide for Small Businesses are available upon request on CD or by download from AXA's small business website (www.axa4business.co.uk).

Important Notice

Publication issued or updated on: 20 January 2012

Ref: 644