

This factsheet will introduce you to Business Continuity Management (BCM), which is a process developed to counteract systems failure. It includes a ten point disaster recovery plan.

CONTENTS

INTRODUCTION

BENEFITS OF BUSINESS CONTINUITY

MANAGEMENT

THE 8 ELEMENTS OF BUSINESS CONTINUITY

BUSINESS CONTINUITY - 10 POINT PLAN

FURTHER HELP AND ADVICE

Business Continuity Management (BCM) is a process developed to counteract systems failure. It is not just about the recovery of IT systems and services, it is an organisation wide discipline. Business continuity management is a business issue, with benefits for any organisation. Supporting the ability of the business to recover is disaster recovery.

This includes:

- Providing facilities and services to enable the business to continue to function
- Providing critical IT applications and infrastructure necessary to support the recovery of critical processes. Underpinning the recovery is crisis management. This ensures that:
 - The most appropriate personnel are brought together to manage the immediate effects and the wider implications of an incident
 - Decisions on what should be recovered (and how this should be done) are made based on information provided by other areas of the business. For example, the IT department, Human Resources, etc

Once a business continuity management plan

has been implemented, it is the start of an ongoing commitment. Organisations constantly evolve and change and recovery strategies must evolve with them. For example:

- Business processes change, people join, transfer and leave organisations on a regular basis. Plans should be updated to reflect changes in recovery teams
- New IT systems are introduced to support business activities. These may be essential and, as such, the requirement to recover them must be considered before implementation
- Ongoing training and testing is vital to ensure effective recovery

This factsheet is for any business that wants to plan a strategy for continuing to operate effectively following a disaster. It covers the benefits of BCM, and a ten point plan to help you implement a disaster recovery operation.

BENEFITS OF BUSINESS CONTINUITY MANAGEMENT

There are real business benefits to be gained from the implementation of business continuity management within any organisation. For example:

- Regulatory requirements
- Positive marketing of contingency capabilities
- Competitive advantage
- Insurance

REGULATORY REQUIREMENTS

In some industries a recovery capability is becoming a mandatory requirement. For example, regulators stipulate that financial organisations must have sufficient continuity and security controls to meet the business requirements. Failure to demonstrate tested recovery facilities could result in heavy fines. Within the service community, there is also an obligation to provide continuous services, for example, hospitals, emergency services and prisons.

POSITIVE MARKETING OF CONTINGENCY CAPABILITIES

An organisation that can demonstrate effective business continuity management capabilities will provide high service levels to clients and customers, and thus win business.

COMPETITIVE ADVANTAGE

The ability to demonstrate contingency provision for systems failure is an increasing requirement when inviting service organisations to tender for business.

A sound business continuity management plan can prove a good incentive for customers to continue a business relationship, and becomes part of the competitive advantage used to win or retain customers.

INSURANCE

Effective business continuity management process can help organisations demonstrate to underwriters or insurers that they are proactively managing their business risks.

The ability to recover the business and mitigate losses is often a requirement of insurance policies. As such, organisations with comprehensive business continuity plans are lower risk, and premiums should reflect this. Alternatively, the organisation may feel

comfortable in reducing cover or even self-insuring certain areas as a result of limiting potential losses.

THE 8 ELEMENTS OF BUSINESS CONTINUITY

There are a number of elements that should be considered for Business Continuity, namely:

1. BUSINESS CONTINUITY MANAGEMENT: PROCESS

The business continuity management process consists of four stages:

- **Stage 1: Initiation**
- **Stage 2: Requirements and strategy**
- **Stage 3: Implementation**
- **Stage 4: Operational management**

The first three stages involve the establishment and implementation of business continuity management within an organisation. The final stage is ongoing operational management of the process.

Stage 1: Initiation

This stage covers the establishment of the business continuity management process, including sponsorship, budget approval and identification of appropriate resources.

Activities to be considered during the initiation process depend on the extent to which business continuity management disciplines have been applied within the organisation.

Some parts of the business may have established individual continuity plans based around manual solutions, whereas IT may have developed contingency plans for systems perceived to be critical.

As part of the project initiation it is essential to scope the initiatives. Careful consideration should also be given to the inclusion of critical third parties.

Stage 2: Requirements and Strategy

This stage provides the foundation for business continuity management and is critical to determine:

- How well an organisation will survive a business interruption or disaster
- Any costs that will be incurred as a result of a business interruption or disaster

Requirements are identified through business impact analysis and risk assessment activities.

In turn, these feed into a business continuity management strategy that proposes risk reduction measures and recovery options, in support of business continuity.

Stage 3: Implementation

Once the business continuity strategy has been agreed (typically by Senior Management or the Board), the business continuity management lifecycle moves into the implementation stage. This stage includes:

- Establishing a business continuity management plan. This should include clear roles and responsibilities for any personnel who will be involved in a recovery
- Developing implementation and supporting plans
- Providing resources to implement risk reduction measures that are detailed in the business continuity strategy
- Procuring recovery facilities
- Proving continuity capability through initial testing

Stage 4: Operational Management

The completion of the first three stages of the business continuity management process will mean that a business continuity management solution has been analysed, agreed and implemented within the organisation. You then need to ensure that the strategy and recovery facilities are maintained as part of

day-to-day business activities.

The business continuity manager has responsibility for maintaining the business continuity management environment through a series of operational management activities.

These activities include:

- Reviews
- Change management
- Education and awareness
- Training
- Testing
- Assurance

2. BUSINESS CONTINUITY MANAGEMENT: IMPACT ANALYSIS

How much does your organisation stand to lose in the event of a disaster or other disruption?

The purpose of a Business Impact Analysis (stage 2 of the business continuity management process, detailed on page 3) is to assess the risk by identifying:

- Critical business processes
- The potential damage or loss that may be caused to the organisation as a result of a disruption to critical business processes

This analysis determines what recovery facilities are provided and ensures that the organisation can allocate business continuity management resources in the most appropriate way.

If a Business Impact Analysis is not undertaken, or is not done correctly, resources may be wasted on unnecessary services that do not fully support a recovery.

What should be included?

Specifically the Business Impact Analysis will identify impacts resulting from an inability to undertake normal business processes. Impacts are measured against particular scenarios for example, the inability to provide call centre services for a period of time.

The impact analysis should concentrate on those scenarios where the impact on critical business processes is likely to be greatest. It will include:

- ‘Hard’ impacts - financial loss, breach of law, regulations, or standards, failure to achieve agreed service levels, increased costs of working
- ‘Soft’ impacts - political, corporate or personal embarrassment, loss of competitive advantage, loss of credibility

Consideration will also be given to how the degree of damage or loss is likely to escalate after a service disruption. This will enable identification of the minimum critical requirements for the continued operation of the business process, and the timescale within which such requirements should be provided. These requirements include:

- The staffing, skills, facilities and services (including the IT applications and data recovery requirements) necessary to enable critical and essential business processes to continue operating at a minimum acceptable level
- The time within which minimum levels of staffing, facilities and services should be recovered
- The time within which all required business processes and supporting staff, facilities and services should be fully recovered

This information can be collected through interviews or workshops with senior members of the business areas. It is important that respondents have a good understanding of their business including an appreciation of dependencies on other departments.

The Business Impact Analysis enables each business area to understand at what point the unavailability of their business process would become untenable within the organisation -

immediately, after a day, week, month or so on. This in turn allows the most appropriate continuity mechanisms to be determined to meet these business requirements.

Other Considerations

The Business Impact Analysis should also consider any implications associated with loss of integrity of information, and for IT systems the impact of the loss of data.

With the move to direct data entry and online transaction processing, consideration of how data will be reconciled is an essential part of the recovery process.

In most cases, business processes can be re-established without a full complement of staff, systems and other facilities, while still maintaining an acceptable level of service to clients and customers. The business recovery objectives should therefore be stated in terms of:

- The time within which a predefined team of core staff and stated minimum facilities must be recovered
- The timetable for recovery of remaining staff and facilities
- The point to which data must be recovered

3. BUSINESS CONTINUITY MANAGEMENT: RISK ANALYSIS

What is the likelihood of a disaster or other serious disruption occurring?

A risk assessment enables an organisation to gauge the level of threat and the extent to which it is vulnerable. These are key factors in determining business continuity management requirements. Activities covered by an assessment should include:

- Identification of risks. For example, damage or denial of access to premises
- Appraisal of the impact of a loss of utilities e.g. electricity, water or gas

- Appraisal of the failure of business partners or service providers
- Appraisal of the impact of single points of failure within the IT infrastructure. For example, reliance on a single gateway for external communication or the unavailability of key staff

A risk assessment should detail threat and vulnerability levels where:

- Threat is defined as "how likely is it that a business disruption will occur?"
- Vulnerability is defined as "whether, and to what extent, the organisation will be affected if a threat materialises"

4. BUSINESS CONTINUITY MANAGEMENT: STRATEGY

The business continuity management strategy is developed using information collated from the business impact analysis and the risk assessment.

The strategy should be presented as a series of options for Senior Management to consider. These options should reflect a balance between risk reduction and recovery.

Defining the options within the strategy is the most important stage of the process. If the requirements gathering is flawed the strategy will be flawed and will not fully support the business recovery.

Options may range from a low-cost strategy such as do nothing if the impacts are minimal or if Management is prepared to accept the risk, to full continuity provision, with obvious cost implications. The latter may be justifiable if:

- Impact is high
- Risks are great

It may be necessary to consider different options for short-term and long-term recovery and all costs and benefits of each option need to be understood before a decision is made. Typically a strategy will fall somewhere between the two and will be a balance of risk reduction and

recovery.

5. BUSINESS CONTINUITY MANAGEMENT: PLANS AND PROCESS

Plan development is one of the most important parts of business continuity management implementation. Without workable plans the process will certainly fail. Plans are needed on three levels, detailed below.

Level 1

At the highest level a crisis management process and plan is needed. This plan will be supported by other plans as necessary including:

- Damage assessment plan
- Salvage plan
- Public relations plan
- Vital records plan

These are used to identify and respond to a service disruption, to ensure the safety of all affected staff members and visitors and to determine whether to implement the business recovery process.

Level 2

This should include key support functions, for example:

- Accommodation and services plan
- Computer systems and network plan
- Telecommunications plan
- Security plan
- Personnel plan
- Finance and administration plan

Level 3

Each critical business area is responsible for the developing a plan to show individuals in recovery teams and a detailed task list for the recovery process. The owners of each plan must ensure that they have identified and agreed support and services required from other parties.

SUMMARY

There are many options for developing plans including traditional word processing documents, database packages or specialist planning and plan development tools. Plans must be easily accessible and distributed to all personnel who have a part to play in a recovery. A useful tip is to create single crib sheets for each team. These might include:

- Who owns the plan and who is responsible for updating it
- General responsibilities
- Assembly points and incident control centres, where applicable
- Departmental strategy
- Members of the recovery team and alternative contact details
- Other useful contacts
- Facilities to be provided at the recovery site
- Action list
- How to get to the recovery site

The IT recovery plan must contain all information needed to recover the computer systems, network and telecommunications in a disaster situation. It must also contain details of how lost data can be recovered and reconciled and how systems can be realigned. The plan should include:

- Systems and applications restoration procedures
- 'Run-books' detailing the order of recovery of applications and data
- Business-driven data reconciliation
- Data integrity checking
- Security permissions

6. BUSINESS CONTINUITY MANAGEMENT: RISK REDUCTION

The requirements analysis will have identified those issues that need to be addressed through risk reduction rather than recovery. These may

include:

- Cross-training for critical or specialist operations
- Changes to business practices to remove or reduce the number of points of failure
- Documentation of critical functions
- Splitting business processes over more than one site
- Installation of UPS (Uninterruptible Power Supply) and potentially back-up power for computer systems to reduce vulnerability to power failure
- Implementation of a more robust backup strategy and tape management system.
- Providing offsite storage of backup media, either within the organisation or with a third party
- Fault-tolerant and/or high-availability systems for critical applications where even minimal downtime is unacceptable. For example, a banking system
- RAID arrays (Redundant Array of Independent Discs) and disc mirroring for LAN (Local Area Network) servers to guard against data loss and to ensure continued availability of data
- Holding spares to be used in the event of equipment or component failure. For example, having a spare LAN server already configured and available to replace a faulty server within a minimum timescale

7. BUSINESS CONTINUITY MANAGEMENT: OPERATIONAL MANAGEMENT

Operational management is the responsibility of the business continuity manager. Activities should include:

- Reviews
- Change Management
- Education and Awareness
- Training
- Testing
- Assurance

Reviews

As organisations can change rapidly, it is necessary to invest in an ongoing review programme. A regular review of all deliverables in the business continuity management process should be undertaken to ensure that they remain current. This will include:

- A review of business processes
- A review of the impacts of systems failure on those processes
- A review of the risks, threats and vulnerabilities to the organisation
- Revision of the recovery measures as required

The business continuity management strategy should be reviewed, generally on an annual basis, to take into account any changes in business direction, business strategy or IT strategy and to consider any updates to the impact analysis and risk assessment.

Business recovery plans will need to be reviewed and updated regularly throughout the year to take account of personnel changes. Update the IT recovery plan whenever there is a major change to IT infrastructure, assets or dependencies such as new systems or networks, or a change in service providers.

Change Management

Incorporating business continuity management into the change management process will ensure that contingency facilities are established before new systems and applications are implemented. It will also ensure that any changes in the infrastructure are reflected in the contingency arrangements provided by IT or third parties. A member of the business continuity team should attend change management meetings on recovery or resilience requirements. Plans should also be updated following tests and reviews, and in response to day-to-day changes. Inaccurate plans and inadequate recovery

capabilities may cause business continuity management to fail. Change management complements the review process and will highlight any issues that have been overlooked.

Education and Awareness

Education and awareness will ensure that all staff are familiar with the implications of business continuity management, and with their roles and responsibilities in a recovery situation. As a consequence, the ability of the organisation to respond better to an incident will be greatly enhanced. This will range from better evacuation procedures, knowledge of assembly points, familiarity with the desk that a recovery team member should occupy during a recovery, etc.

Training

It is vital that all personnel involved in the implementation and maintenance of business continuity management are fully trained and can undertake their responsibilities effectively. IT staff need to be trained in the necessary procedures to ensure that they can recover systems and applications quickly and efficiently. In addition, other types of training may be considered appropriate. For example: media training for senior managers or trauma counselling training for Human Resources staff.

Testing

Establish a regular programme to ensure that the critical components of the strategy are tested at least annually, or as directed by senior management or audit.

It is important that any changes to the IT infrastructure are included in the strategy, implemented in an appropriate fashion and tested to ensure that they function correctly. Continual testing of the effectiveness of the recovery teams is also essential so that staff

remain aware of their responsibilities. It is also important to ensure that new members of the recovery team are familiar with their individual roles.

Assurance

The final activity in operational management involves obtaining assurance that the quality of the business continuity management deliverables is acceptable to senior business management, and that the operational management processes are working satisfactorily. This should be undertaken as part of the internal and external audit process and can be used to demonstrate the effectiveness of the business continuity management environment.

8. BUSINESS CONTINUITY MANAGEMENT: TESTING

The purpose of testing is to:

- Raise the level of confidence in the ability to recover from a systems failure
- Raise awareness and implement training processes within the organisation as early as possible

An initial technical test can usually be completed without the need to involve the business. However, for subsequent tests it is prudent to involve the business as a whole. This will help to improve capability, and aid mutual understanding of the activities and resources needed to achieve the common goal of business recovery.

A full technical test will replicate as far as possible the stand-by arrangements, including the recovery of business processes and the involvement of external parties. This should test completeness of the plans and confirm:

- Time objectives. For example, time taken to recover key server applications
- Staff preparation and awareness
- Staff duplication and potential over-

commitment of key resources. For example, a systems administrator being required to support a number of modular plans (help desk, operations, networks and communications)

- Responsiveness, effectiveness and awareness of third parties and service providers

It is also necessary to ensure that the business recovery teams are tested. This can include familiarisation with the recovery site, and the provision of examples that will test the team response to a relevant scenario.

All tests, whether technical or non-technical, must have clearly defined objectives and critical success factors which will be used to determine the success or otherwise of each exercise.

BUSINESS CONTINUITY - 10 POINT PLAN

The following ten-point plan is included as a reminder for the business continuity management process. The Business Continuity Institute (BCI) and the Disaster Recovery Institute International (DRII) have identified these areas as being key to effective business continuity planning.

Project initiation and management

- Has a business continuity manager been identified?
- Have support and sponsorship from senior management been achieved?
- Has a management structure been established?

Risk evaluation and control

- Has a risk assessment been undertaken?
- Have risk reduction measures been identified to mitigate potential losses?

Business impact analysis

- Have critical business processes been established?

- Have the impacts of losses been identified?
- Are interdependencies between departments known?
- Can prioritisation and time dependencies of business processes be achieved?

Developing business continuity strategies

- Have all critical processes been identified and recovery timeframes agreed?
- Has the strategy considered both recovery and risk reduction?
- Is the strategy appropriate to the business and are critical operating requirements supported?

Emergency response and operations

- Has a crisis management process been established to respond to incidents?
- Are all team members aware of their responsibilities?

Developing and implementing business continuity plans

- Have business continuity plans been developed in support of the strategy?
- Are these plans owned and managed by the business?

Awareness and training plans

- Have all staff been made aware of business continuity management and is this promoted as an ongoing initiative?
- Have recovery teams been trained in their roles and responsibilities?
- Are IT and other specialist groups aware of their expected response to an incident and can they effectively provide the support required?

Maintaining and exercising business continuity plans

- Are all business continuity plans and supporting procedures owned by a nominated

business or support person?

- Is plan maintenance undertaken on a regular basis?
- Has a test strategy been developed with exercises and tests undertaken on a regular basis?
- Are plans updated to reflect changes in business strategy?

Public relations and crisis coordination

- Does the crisis management process include internal and external communications, the media and potentially, trauma counselling?
- Is a process in place to ensure that all stakeholders are kept informed on a 'need-to-know' basis?

Co-ordination with public authorities

- Have local authorities and emergency services been included in the plans?
- Have procedures and policies been developed to ensure compliance with applicable statutes or regulations?

FURTHER HELP AND ADVICE

Information Providers

The Business Continuity Institute (BCI)

<http://www.thebci.org/>

Disaster Recovery Institute International (DRII)

<http://www.drii.org/>

GENERAL BUSINESS ADVICE

For more information on achieving best practice in your business contact your local Business Link advisor by visiting the website at

<http://www.businesslink.gov.uk> or calling 0845 600 9 006.

Published by the Department of Trade and

Industry. <http://www.dti.gov.uk> © Crown Copyright