Business Continuity Planning for Major Disruptions
Checklist 255

Introduction

Major disruptions to organisations come in many forms. Extreme weather conditions, technical failure, people related factors such as increased unplanned absences, security breaches and supply chain incidents are all examples of events that can cause business disruption. Without pre-prepared systems; continuity and recovery plans; and trained people in place, organisations can be irreversibly damaged as a consequence of business operations downtime, and the resulting suspension of the delivery of services and products to customers.

In order to ensure that organisations are equipped to effectively identify, manage, respond and recover from major disruptions, it is essential that a Business Continuity Management (BCM) framework is in place. This checklist outlines the key components of the framework which collectively safeguards companies from harmful threats.

Definition

Disaster planning, crisis management, business continuity, disaster recovery – these are just some of the naming conventions used historically and internationally for several elements that play a part in a BCM framework. Collectively, the group of business continuity planning competencies required to respond to a threat, reinstate continuity, and then subsequently deliver full restoration is known as Business Continuity Management (BCM).

The British Standards Institution Code of Practice for Business Continuity Management, BS25999-1, defines BCM as:

An holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creation.

Action checklist

1.   Understand the components of the BCM framework

The essential building blocks of a BCM framework consist of:

- BCM programme management – e.g. establishing elements such as programme scope, objectives, roles and responsibilities
- understanding the organisation and the impact identified threats would present

- determining the BCM strategy
- developing and implementing the BCM response
- exercising, maintaining and reviewing the BCM framework to ensure it remains fit for purpose at all times
- embedding BCM in the organisation's culture.

2.   Gain support from senior management

The scope of the BCM programme needs to be determined and owned by senior managers. This ensures that the activities required to deliver and implement the programme are fully supported from the top down. It also ensures that the programme is delivered in accordance with the needs of the organisation from a strategic and operational perspective.

3.   Outline the scope of the BCM programme

The scope of a BCM programme must be determined by the objectives and outputs it needs to deliver.

Considerations regarding scope may include the following:

- whether to include the core organisation only or include all outsourced partners (managed services, supply chain, resellers)
- whether to include the whole organisation or just critical processes or departments within it
- whether to include all of the technical IT and telecommunications infrastructure or just critical dependencies for specific areas of the organisation.

4.   Allocate roles and responsibilities

For effective BCM programme management to be achieved; roles and responsibilities must be clearly assigned, approved by senior management, and methods for reporting progress must be agreed and understood. Ongoing owners or champions for every element of the system must also be established to ensure smooth delivery and maintenance of the programme across the organisation.

5.   Understanding the Organisation

Based on the agreed scope of the BCM programme, the impact on the operations of the organisation if pre-established threats were to materialise needs to be determined. Undertaking Business Impact Analysis (BIA) and Risk Assessment activities (See sections below) will provide an understanding of the organisation and assist you in developing its capability to manage business continuity.

The personnel required to provide information for BIA and Risk Assessment activities should be carefully selected for their knowledge and expertise before embarking on a work stream of sequential individual and group exploration activities. This ensures the best use of the time contributed to the programme by all involved, as well as promoting the programme in a positive way.

5.1.   Undertake Business Impact Analysis (BIA) activities

Business Impact Analysis targeted activities are conducted to:

- identify your organisation's critical products and services
- identify the critical processes and procedures that cumulatively deliver each product and service
- establish how the suspension of these activities will affect the organisation over an increasing time period (typically ranging from 24 hours through to 4 weeks). Operational, strategic, financial and reputation impact are criteria commonly used to assess impact during BIA activities
- establish the organisation's maximum threshold for the suspension of these activities, i.e. the point at which continued suspension may lead to potentially serious or irreversible damage to the organisation
- establish the resources required to recover data, people-knowledge, IT systems, bespoke equipment, suppliers, etc.
- establish known recovery capabilities and timeframes.

All of this information should be fully captured through a process of methodical questioning, and where possible, reviewing any evidence provided in support of the answers given. The information attained (along with Risk Assessment data) can then be presented to senior management so that BCM strategies can be agreed. This will also shape the direction of the BCM programme and the activities to be undertaken. The activities involved in undertaking a BIA and Risk Assessment will enable you to understand your organisation better and to build your BCM capability.

5.2.　Carry out Risk Assessment activities

Agree the types of risk for exploration such as the loss of IT and communications or critical suppliers (as examples) with the BCM programme working group before embarking on Risk Assessment activities.

Conduct risk assessment activities to determine the likelihood and impact of these agreed risk types (if they materialised) in terms of fully/partly suspending the organisation, affecting both the delivery of business critical products and services, as well as disrupting critical processes and procedures as identified in the BIA stage in section 5.1 above (such as the preparation and running of payroll for example).

5.3.　Consider mitigation options

Once all risk assessment activities have been undertaken and there is an understanding of the likelihood and impact of the risks materialising in relation to each critical element identified in the BIA, the next activity is to look at the mitigation options available in order to reduce their likelihood and/or impact (and resulting associated impacts to the organisation). The mitigation options typically are:

- **Transfer** – i.e. outsource the root cause so that a third party carries the risk
- **Reduce** – apply risk treatment techniques such as preparing for the risk materialising by developing specific business continuity plans to recover from it
- **Terminate** – look at re-engineering a process where certain risks are currently present
- **Accept** – do nothing and hope the risk never materialises.

6.　Determine BCM strategies

This element of the BCM programme provides the continuity strategies available for the maintained delivery of the critical products and services when major disruptions suspend/part-suspend them.

Having already established known recovery capabilities and timeframes for each of these during Business Impact Analysis activities, the actual continuity strategies and resources required to achieve the required restoration timeframes now need to be agreed by Senior Management and subsequently documented.

Examples of BCM strategies may include the following:

- **People** – critical processes are documented and other staff members are then cross-skilled to be able to deliver them
- **Premises** – provisioning alternative sites or facilitating remote working
- **Technology** – splitting technology infrastructure across multiple connected sites
- **Information** – critical back-up data is maintained and stored remotely for prompt retrieval and loading
- **Suppliers** – alternative 'stand-by' sourcing channels are identified.

All approved continuity strategies should be captured within business continuity and technical disaster recovery documentation.

7.　Develop and implement the BCM response

This stage of the BCM programme focuses on the how, what and who, when recovering the organisation's critical operations following a major disruption. In order for effective recovery and continuity to take place, incident management systems need to be defined, processes created, and appropriate plans written.

7.1.   Clarify the roles and responsibilities of the Incident Management Team

It is essential to have a clear understanding of the triggers which will invoke the incident management response and of who will be responsible for assessing incidents and taking prompt decisions on whether the incident management team should be called upon. Members of the incident management team need to be identified and prepared to perform their roles, both as individuals and as part of a team. Duties should be allotted to each member ahead of a major incident occurring. Make sure that the protection and preservation of life is the number one priority for the incident team. To ensure that this happens, integrate health and safety procedures within business continuity plans. This will mean that building evacuation, the provision of first aid (and potentially counselling services for staff if these are contracted), are automatically worked through as part of the incident management team's task list.

7.2.   Draw up Business Continuity Plan(s)

Critically, business continuity plans provide direction and support information to the incident management team to:

- recover the critical products and services within the timescales and priority order required (working within the maximum time thresholds the organisation can tolerate before potentially irreversible damage is caused)
- mobilise and direct the resources required to achieve continuity and recovery
- maintain the reputation of the organisation throughout the event through managed communications internally and externally
- engage coherently with third parties such as suppliers and/or emergency services as required
- maintain the confidence of employees through demonstrating that their wellbeing has been provided for and considered at all times
- present assurances to customers that business disruption is being managed professionally to restore normal services in the shortest possible time and with the minimum of inconvenience caused.

Business continuity plans can be single documents consisting of many different sections, or may be standalone documents that serve a specific purpose, such as the communications plan, for example. Each plan should include the methodology detailing how the document would be invoked and accessed as part of the incident management team invocation process. It should also clearly state its purpose and scope. If the plan is one of a suite of plans then all relationships with other plans should be stated within the document along with information relating to the author and owner of each appropriately.

'Major Incident' communications stakeholder audiences need to be established externally as well as internally for completeness; ensuring that messages are appropriate to each audience and are consistent across all message platforms (such as customer facing Internet pages) throughout the management of the recovery cycle. These communication requirements can be written as a standalone Communications Plan or can be added as a section of a larger Business Continuity Plan.

Business continuity plans should be self-explanatory, avoiding the use of unnecessary jargon. Sequential activities to achieve continuity and recovery should be included (to achieve the deliverables stated in the purpose and scope of the plan), with each activity pre-assigned to the individual roles that make up the incident management team. Remember that business continuity plans are only as good as the information contained within them so they should be regularly reviewed, maintained and revised as part of business as usual document version control.

8.   Exercise, maintain and review the BCM framework

Exercising, maintaining and reviewing the BCM framework is essential if organisations are to remain fully prepared. This can be achieved using a variety of different methodologies:

- **Testing** – where specific elements of your systems or plans are tested in isolation such as the incident management team invocation process
- **Discussion based** – where instrumental groups of people are invited to workshops to walk through the business continuity plan(s) and concerns and assumptions are highlighted immediately
- **Table top** – these are 'virtual' events delivered to test systems, rehearse people and exercise plans against scenarios which an organisation is known to be subject to

- **Live** – these are generally conducted when the three above alternatives would not capable of providing real data enabling any needs for preparedness improvements to be established. Live exercising has the potential to impact the organisation detrimentally if not controlled and implemented properly. As such it requires a greater degree of planning and control than the other methodologies.

Exercises should be performed at least annually. However, the frequency will be dictated by such things as business change, regulatory requirements, licensing requirements, and supply chain agreements, etc. Maintain the framework by ensuring that plans are updated if critical services or products are changed for example.

9.   Embed BCM in the organisation's culture

It is essential to embed BCM into the organisation's everyday business operations. Ensure that all employees understand what their responsibilities are for reporting incidents. Also make certain that employees feel assured that the organisation is best prepared to manage major incidents should they arise. Raising the awareness of the BCM framework across the organisation can be simply achieved by providing regular information using internal media – intranet, emails, notice boards, etc. – as well as communicating any scheduled exercises that are taking place. All employees need to understand who is responsible for the implementation of the BCM framework and as such, an open door policy for two-way information exchange should always be promoted.

BCM also needs to be incorporated into business change processes. Any changes in the way an organisation conducts its business operations, through new projects, fresh supply chain relationships, or changes to its portfolio of products and services, for example, will have implications for the effectiveness of business continuity plans and these should be considered to ensure that the organisation remains prepared at all times.

Potential Pitfalls

Managers should avoid:

- being complacent – disasters are usually unexpected. It could happen to you!
- assuming you've thought of everything – listen carefully to comments and suggestions
- forgetting to test your plans
- letting your plans get out of date.

Additional resources

Books

Managing business risk: a practical guide to protecting your business, 8th ed., Jonathan Reuvid
London: Kogan Page, 2012

Weathering the storm: the 2013 business continuity management survey, Ben Musgrave and Patrick Woodman,
London: Chartered Management Institute, 2013

Business continuity management: a practical guide, Stuart Hotchkiss
Swindon: British Informatics Society, 2010

Business continuity management: a crisis management approach, 2nd ed., Dominic Elliott, Ethne Swartz, Brahim Herbane
New York NY: Routledge, 2010
This book is available as an e-book.

This is a selection of books available for loan to members from CMI's library. More information at: www.managers.org.uk/library

Organisations

The Business Continuity Institute, 10 Southview Park, Marsack Street, Caversham, RG4 5AF
Tel: 0118 947 8215 Web: www.thebci.org

Related checklists

Performing a SWOT analysis (005)
Health and safety: fire precautions planning (184)

National Occupational Standards for Management and Leadership

This checklist has relevance to the following standards:
LB: Manage risks to your organisation, unit B1
LB: Develop, maintain and evaluate business continuity plans and arrangements, unit B2

This is one of many checklists available to all CMI members. For more information please contact

t: 01536 204222   **e**: enquiries@managers.org.uk   **w**: www.managers.org.uk

Chartered Management Institute
Management House, Cottingham Road, Corby NN17 1TT.

This publication is for general guidance only. The publisher and expert contributors disclaim all liability for any errors or omissions. You should make appropriate inquiries and seek appropriate advice before making any business, legal or other decisions. Where legal or regulatory frameworks or references are mentioned these relate to the UK only.

May 2013