



**BUSINESS CONTINUITY
INSTITUTE**

**GOOD PRACTICE GUIDELINES
2008**

*A Management Guide to Implementing
Global Good Practice in
Business Continuity Management*

**SECTION 1
BCM POLICY & PROGRAMME
MANAGEMENT**

ABOUT THIS GUIDE

1. Introduction

The BCI published its first Good Practice Guidelines in 2002. This played a significant part in the development of the British Standards Institution's (BSI) Publicly Available Specification for Business Continuity Management (PAS 56). GPG05 was issued followed by an extensive rewrite in to take into account the latest thinking in BCM internationally and to recognise increasing maturity in BCM practice across all sectors, public and private.

This guide follows the structure of BS25999-1:2006 A Code of Practice for Business Continuity Management published by the British Standards Institution and can be viewed as an implementation guide and a definitive text for those wishing to understand BCM principles and practices in a more comprehensive manner. Key requirements for certification in BS 25999-2:2007 Specification for Business Continuity Management are identified in this guide but the standard should be consulted for the complete set of requirements.

There is a close relationship between the structure of this GPG and BS 25999-1 because the BCI GPG has always been a key component of BSI initiatives in the BCM field. However as a global institute, The BCI needs to reflect good practice across the world. BS25999 offers a comprehensive view of the subject but there are other standards in place with which many BCI professional members need to understand. As such the GPG07 is also designed to cover the main requirements of NFPA1600 (US and Canada) HB221 (Australia), APS 232 (Australia) and FSA (UK).

In no cases, however, must the GPG be seen as a replacement for those standards or as a guarantee of compliance with those standards.

2. Objective

This document is intended to provide an overview and guidance on good practice covering the whole Business Continuity Management (BCM) Lifecycle from the initial recognition of the need for the development of the programme to the on-going maintenance of a mature Business Continuity capability.

It is intended that standard bodies define the requirements of a BCM programme and that where the Code of Practice calls for a process, these Guidelines provide more detail on how that process may be undertaken. However, being a procedure guide there are, in places, additional steps identified in the Guidelines that are necessary to undertake to implement the requirements of any Standard.

3. Audience

These Guidelines draw upon the considerable academic, technical and practical experiences of the members of the Business Continuity Institute - that is practitioners who have both developed and shaped the guidelines in the real world.

These guidelines are therefore intended for use by BCM practitioners, risk managers, auditors and regulators with a working knowledge of BCM principles. They are not intended to be a beginner's guide. Newcomers to the discipline should work alongside an experienced practitioner or attend an appropriate education programme.

The principles in these guidelines are applicable to all organisations of any size, sector and location - from those with a single site to those with a global presence.

4. Acknowledgments

The GPG08 is edited by Lyndon Bird FBCI and the principle author is Ian Charters FBCI.

This Guide is derived from BCI GPG05, to which the people listed below contributed.

Anne Wright MBCI	Howard Booth MBCI
Ian Griffiths MBCI	Helen Sweet ABCI
Richard Ecclestone SBCI	John Worthington MBCI
Martin Lippiett MBCI	Mel Gosling MBCI
James Coates MBCI	Mark Mahoney MBCI
Michael Bland MCBI	David Bennett MBCI
Jim Barrow MBCI	Elaine Weston MBCI
Julia Graham FBCI	Colin Ive MBCI
Michael Bews MBCI	Adrian Jolly
Jane Naylor	Richard Bridgeford MBCI
Andy Tomkinson MBCI	Angela Hobley MBCI
Jo Welland	Nathan Bird MBCI
Jeanette O'Neil MBCI	Ian Charters FBCI

The Business Continuity Institute acknowledges the time and expertise voluntarily given by all those listed above to the development of the Good Practice Guidelines for the benefit of the BCI and the Business Continuity Industry. Contributors to the guidelines have freely donated their copyright and IP rights to the Business Continuity Institute so that the Institute will be able to ensure that the guidelines remain current and complete.

5. Version History

<i>Year</i>	<i>Version</i>	<i>Date</i>	<i>Summary of changes</i>
2007	1	January	First issue
2007	2	March	Major reorganisation and update to support BS 25999-1
2007	3	October	Minor corrections & BCI logo changes BCM indicators removed
2008	1	January	New entry for BCMS & PDCA. BS 25999-2 references
2008	2	November	Relatively minor amendments to its format and presentation

Format of this Guide

The Guide has been prepared in 6 sections, which are in line with the earlier versions of the Guide and also with BS25999 nomenclature.

Section 1 consists of the Introductory Information plus BCM Policy & Programme Management

Section 2 is Understanding the Organisation

Section 3 is Determining BCM Strategy

Section 4 is Developing and Implementing BCM Response

Section 5 is Exercising, Maintaining & Reviewing BCM arrangements

Section 6 is Embedding BCM in the Organisation's Culture

6. BCM Professional Qualifications

For those individuals who wish to become professional members of the BCI, competence needs to be shown in 6 subject matter expertise areas. These are compatible with the BCM Lifecycle, supported by the BCI and now form an integral part of BS2599. Other certification bodies might still use an older version of professional competences which include 10 skill requirements. A skills map is provided as an appendix to Section 6 that shows the relationship of the 10 skills to the knowledge requirement of the GPG.

INTRODUCTION

1. What is Business Continuity Management?

Business Continuity Management (BCM) is an holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

BCM must be owned and fully integrated into the organisation as an embedded management process.

BCM aims to improve an organisation's resilience. By identifying, in advance, the potential impacts of a wide variety of sudden disruptions to the organisation's ability to succeed it is able to prioritise the efforts of various other specialists aiming to achieve resilience in their areas of expertise such as security, facilities and IT.

While concerned with all scales of resilience, BCM is particularly concerned with developing organisation-wide resilience allowing an organisation to survive the loss of part or all of its operational capability. It should also look at surviving significant losses of resources such as staff or equipment. Because an organisation's BCM resilience depends on its management and operational staff as well as technology and geographical diversity, this resilience must be developed throughout the organisation from senior management to shop floor and across all sites and the supply chain.

The driver for this organisational resilience is the responsibility the senior management have for the long-term interests of the staff, customers and all those who depend on the organisation in some way. Whilst it may be possible to calculate the financial losses of disruption the most significant impact is usually in damaged reputation or loss of trust that results from a mismanaged incident. Conversely a well-managed incident can enhance the reputation of the organisation and its management team.

2. The Case for Business Continuity Management

"It won't happen to us", "We will cope - we always do", "We are too big to fail" and "We are not a terrorist target" are frequent responses by businesses when questioned about their lack of preparedness. Others believe their insurance company will pay for everything. Most think they haven't got the time to prepare for something that will never happen. The catalogue of businesses that have failed following an incident suggests that these responses are based on false assumptions.

Whilst bombs, fires and floods capture the headlines almost 90% of business-threatening incidents are 'quiet catastrophes' which go unreported in the media but can have a devastating impact on an organisation's ability to function. Many of the causes are outside of an organisation's control and they are often at the mercy of the emergency services or suppliers who define the timescale of an interruption.

In managing any event, a successful outcome is judged by both the technical response and the perceived competence of the management. Research by Knight and Pretty of Oxford Metrica (The Impact of Catastrophes on Shareholders Value by Rory F. Knight and Deborah J. Pretty Templeton College of Oxford University, 1996) indicates that organisations affected by catastrophes fall into two distinct groups - "recoverers" and "non-recoverers". Where an organisation has successfully dealt with a crisis their share value has increased in the long-term in contrast to those who were perceived not to have managed the crisis well whose share price declined and, after a year, had still not recovered. More recent research has shown that those organisations which budget most on risk, BCM and governance are the most profitable companies in their sector suggesting that BCM is an investment not a cost.

A key feature of successful BCM programmes is that ownership of the various responsibilities has been taken at the appropriate levels in the organisation. In these organisations BCM implications are considered at all stages of the development process of new projects and the BCM implications are part of the change control process.

3. How will it benefit my organisation?

The main purpose of BCM is to ensure that the organisation has a response to major disruptions that threaten its survival. Whilst this must be worthwhile in itself, there are other benefits that can be gained by embracing BCM as a management discipline.

Some organisations have statutory and regulatory requirements either specifically for BCM or more generally for 'risk management' as part of their corporate governance requirement. An appropriate BCM plan will satisfy both the specific requirements and contribute both a response to specific risks and to the overall 'risk awareness' of an organisation. However the primary driver for BCM should always be that it is undertaken because it adds value to an organisation and the products and services it delivers rather than because of governance or regulatory considerations.

"For many companies, BCM will address some...key risks and help them achieve compliance".
Nigel Turnbull, Chairman of Turnbull Committee on UK Corporate Governance.

Businesses selling to other businesses have used BCM as a competitive advantage to gain new customers and to improve margins by using it as a demonstration of 'customer care'.

A thorough review of the business through Business Impact Assessment and Plan exercises can highlight business inefficiencies and focus on priorities that would not otherwise have come to light.

Organisations providing services or goods recognise that keeping customers through a more reliable service is cheaper than tempting back deserters after an interruption.

The esprit de corps generated during the successful management of an incident can improve business performance well after the problem has been solved

"I am often asked what single piece of advice I can recommend that would be most helpful to the business community. My answer is a simple, but effective, business continuity plan that is regularly reviewed and tested." Extract of speech by Eliza Manningham-Buller, former Director-General of MI5, to the UK CBI Conference, November 2004.

4. Relationship with other specialist disciplines

Defining what is the responsibility of the Business Continuity Management role within a particular organisation is influenced by the context of the allocation of responsibility to an individual as well as the jobholder's past experience. This may mean that an individual Business Continuity Manager sees security, IT availability or risk management as the key issue with other areas taking a less prominent role. This is why it is so difficult to reach a consensus as to the general description of specifically BCM responsibilities. In particular the relationship with Risk Management is fiercely debated.

These Guidelines take the view that, though they are complementary disciplines, the focus and methods of Business Continuity differ significantly from that of Risk Management. The table below attempts to contrast these approaches.

Table: Comparison of Risk Management and Business Continuity Management

	Risk Management	Business Continuity Management
Key method	Risk Analysis	Business Impact Analysis
Key parameters	Impact & Probability	Impact and Time
Type of incident	All types of events - though usually segmented	Events causing significant business disruption
Size of events	All sizes (costs) of events- though usually segmented	Strategy is planned to cope with Survival-threatening incidents but can manage any size of incident
Scope	Focus primarily on management of risks to core-business objectives	Focus mainly on incident management mostly outside the core competencies of the business
Intensity	All from gradual to sudden	Sudden or rapid events (though response may also be appropriate if a creeping incident becomes severe)

The view presented in these Guidelines attempts to present the core discipline of Business Continuity Management while recognising that individual practitioners are often required, by common sense or direction, to extend their role because of the situation in the organisation they work for.

5. Relationship with other guidelines and standards

The relationship between the GPG07, BS 25999-1 and other national BCM standards has been outlined earlier.

Other standards with BCM elements are:

- PAS 77 IT Service Continuity (soon to be replaced by BS 25777)
- ISO 17799/27001 - Although primarily an information security standard there are aspects of Business Continuity provision which must be covered in order for this standard to be fully implemented.
- ITIL - This standard concerns itself with the provision of Service Management disciplines for example Risk and Security, Change, Problem, Configuration, Capacity and Availability however there is a link between the ITIL IT Service Continuity (Disaster Recovery) and Business Continuity.
- ISO/PAS 23399 - Societal Security (in draft)
- ISO 31000 & BS 31100 - Risk Management (in draft)
- NFP1600
- Data Protection legislation

- Freedom of information legislation
- Health and Safety legislation
- Rules and Guidelines such as those outlined in Sarbanes-Oxley and Basle II, influence BCM by mandating its implementation and setting service continuity parameters

6. How to use these Guidelines

Every organisation is different; it is run in different ways, is sited in different locations and it changes over time. Therefore it is not possible to be prescriptive about the solutions that an organisation should adopt.

The approach of these guidelines is therefore to outline a process and to suggest methods on the assumption that an appropriate solution will emerge if the correct process is followed.

Even so it is recognised that there may be a case where the process outlined may need to be modified to meet the specific needs of an organisation. Therefore each organisation needs to assess how to apply the guidelines to their own organisation. They must ensure that their BCM competence and capability is appropriate to the nature, scale and complexity of their business, and reflects their individual culture and operating environment.

The definition of 'Good' practice implies that there is 'Better' practice, but unlike most other standards, there is a sense in which there is an 'Appropriate' solution for each organisation. To provide less than this risks failure of the entire strategy, but to do more than this is wasteful (of time or money) that could be better utilised elsewhere. Unfortunately this ideal 'appropriate' strategy is difficult to determine exactly but following these Guidelines should provide a systematic approach to identifying where it lies.

7. Scope of the Guidelines

Analysis of the response of organisations to Business Continuity incidents shows that those who cope best have integrated their response across the organisation. In practice this means that the Incident Management capability of the senior management team is supported by Business Continuity logistics and the technical support for resumption.

The Guidelines therefore focus on the primary role of the BCM practitioner and assume that specialist in other disciplines (IT, security, HR and the business) will be available to advise on the implementation of these other aspects.

8. Layout of the Guidelines

The Guidelines first address the BCM Policy and Management issues which set the context and scope of the Programme, then follows the Business Continuity Management Life Cycle; from **Programme Management through Understanding the Organisation**. It then follows the lifecycle elements in a logical fashion - completing with the ongoing component of a BCM programme **Embedding BCM in the organisation's culture**.

There are references throughout to the relevant sections of BS 25999-1 though there is not a one-to-one relationship between the sections.

The Guidelines demonstrate how the stages fit together intellectually; in practice the experienced practitioner will not necessarily follow this progression strictly. For example a 'scenario-based' exercise may provide 'buy-in' at the start of a programme and plans may be written to provide some incident management capability for the organisation before resumption requirements for activities have been investigated. However progress should always be measured against the whole life cycle and across the whole organisation.

9. Structure of the Guideline Content

Each stage contains:

<i>Guideline Stage</i>	<i>Questions answered</i>
Introduction	
Components Details	Contents described below
Key BCM Indicators	What is most important to have done

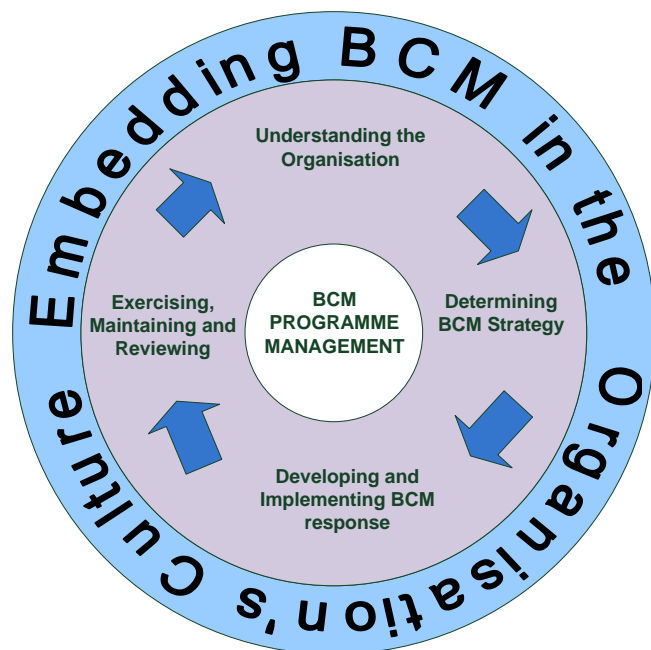
The structure and format of each component follows a common pattern:

<i>Guideline Component</i>	<i>Questions answered</i>
Introduction	
Precursors	What needs to be done before this?
Purpose	Why do we need to do it? What will it achieve?
Concepts and Assumptions	What do we need to understand? What assumptions are we making?
Process	What do we need to do?
Methods and Techniques	What are the tools we need to do it?
Outcomes and Deliverables	What should it produce?
Review	When should it be done?

10. Diagram and Glossary

These guidelines, unlike previous versions of the GPG, use the schematic diagram and glossary from BS25999-1. For official copies of these refer to the BS25999 official standard documentation.

Figure: The BCM Lifecycle—BS 25999-1



11. BCMS and PDCA (BS 25999-2)

BS 25999-2 Specification for BCM introduced the concept of a Business Continuity Management System (BCMS). The 'System' suffix is for consistency with other management systems such as the Information Management System in ISO 27001 and similar Systems for Quality and Environmental Management.

A management system is defined as 'that part of the overall management system (of the organisation) that establishes, implements, operates, monitors, reviews, maintains and improves business continuity'. This implies that the system has:

- A policy
- People with defined responsibility for BCM
- Management processes to support the policy
- A set of documentation - to provide evidence to the audit process
- Specific processes to support the BCM programme
- Resources - including budget, time and facilities

BS 25999-2 also embraces the Plan-Do-Check-Act (PDCA) cycle in common with the other management systems. This relates at a high level to this guide as shown in the table below:

Plan	Establishment of the policy, objectives and scope of the programme - Section 1a
Do	Implementation of the BCM programme - Section 1b, 2 - 6
Check	Internal audit and management review of the BCMS - not covered
Act	Implementation of the results of the review - not covered

The audit and management review in the last two steps of BS 25999-2 are not described in this guide because they specify audit procedures and guidance rather than BCM requirements.

Though the standard is intended to be applicable to all organisations, there is a clear intention not to imply that a BCMS must be of a uniform design. It is up to each organisation to design a BCMS that is appropriate to its needs and stakeholder requirements.

Certification of an organisation does not guarantee that it will successfully manage all disruptions, only the aspects of the process of BCM that can be objectively audited have been carried out.

Organisations seeking suppliers who have achieved BS 25999-2 certification should check that the scope of the certification covers the products and services they are looking to purchase.

GUIDELINES STAGE 1:
BUSINESS CONTINUITY POLICY & PROGRAMME
MANAGEMENT

COMPONENTS

<i>1a. THE BUSINESS CONTINUITY MANAGEMENT POLICY</i>	<i>12</i>
<i>1a.1 REFLECTING ORGANISATIONAL CONTEXT</i>	<i>13</i>
<i>1a.2 BCM POLICY CONTENTS</i>	<i>16</i>
<i>1a.3 BCM PROGRAMME SCOPE & DETERMINING CHOICES</i>	<i>18</i>
<i>1a.4 OUTSOURCED ACTIVITIES</i>	<i>24</i>
<i>1b. PROGRAMME MANAGEMENT</i>	<i>26</i>
<i>1b.1 ASSIGNING RESPONSIBILITIES</i>	<i>27</i>
<i>1b.2 IMPLEMENTING BCM IN THE ORGANISATION</i>	<i>29</i>
<i>1b.3 PROJECT MANAGEMENT</i>	<i>31</i>
<i>1b.4 ONGOING BC MANAGEMENT</i>	<i>33</i>
<i>1b.5 DOCUMENTATION</i>	<i>35</i>
<i>1b.6 INCIDENT READINESS & RESPONSE</i>	<i>37</i>

1a. THE BUSINESS CONTINUITY MANAGEMENT POLICY

Ref: BS 25999-1 Section 4

1. Introduction

The BCM Policy is the key document which sets out the scope and governance of the BCM programme. The Policy provides the context in which the BCM team implement the required capabilities.

When an organisation embarks on a BCM programme it will not have a BCM Policy in place nor, probably, understand the decisions it needs to make to write one. A series of iterative activities is required which work towards a formulation of this Policy. Key steps are:

- Ensuring that the BCM programme supports the objectives and culture of the organisation
- Deciding on the scope of the BCM Programme
- Formulating a BCM Policy

A project or series of projects should be initiated to enable the organisation to develop a Policy and undertake the activities required to implement it.

1a.1 REFLECTING ORGANISATIONAL CONTEXT

Ref: BS 25999-1 Section 4.2 & BS 25999-2 Section 3.2.1

1. Introduction

To be able to develop an appropriate Business Continuity Management programme you must ensure that it reflects organisational objectives and culture

These questions need to be asked:

- What are the objectives of the organisation?
- How are the business objectives achieved?

In some organisations a high level risk assessment of risks that might threaten the achievement of an organisation's strategic and operational objectives will be undertaken as part of the business planning processes. The output of this exercise can provide a useful input when setting the overall context for the Business Impact Analysis. In some regulated environments this Risk Assessment is a mandated activity.

2. Precursors

It is easier to ensure that BCM Policy is aligned to organisational requirements if these are formally identified and agreed.

3. Purpose

The purpose of aligning Business Continuity to the organisation's overall strategy at the start is to:

- Understand the direction and focus of the business before embarking on business impact or risk assessment activity
- Help understand the business plan for growth / downsize, restructure, etc., in the short, medium or long term. This type of information may not be visible to the person charged with business continuity activity and is very much dependent on the type and size of organisation being planned for. Knowledge of business plans will assist in developing recommendations on suitable and flexible contingency strategies.
- To set the geographic scale parameter for the choice of recovery options

4. Concepts and Assumptions

Using a BIA to review the organisation's strategy

It is possible, and desirable, that a BIA is used to determine the impact of interruption in advance of major business restructure such as:

- Introduction of a new product, process or technology
- Office relocation or a change in the geographical spread of the business
- Significant change in business operations, structure or staffing levels
- A significant new supplier or outsourcing contract

This may result in a revision to its implementation or even a reconsideration of the restructure.

5. Process

Market conditions

The reaction of customers and competitors is a key factor affecting the viability of an

organisation after a disruption. Relevant conditions include:

- Whether the product is available from many suppliers, a few or only one
- What is the likely timescale within which alternative suppliers can be found
- Whether within the sector other suppliers will act to take advantage of a company in difficulty or are likely to support one another (which they may do to protect the reputation of the sector)

The BCM Programme could provide a business opportunity to a commercial organisation if the customer is prepared to pay a premium for improved reliance on delivery.

Organisational strategy

Aspects of the organisation's strategy likely to affect the BCM Programme are:

- Expansion (or contraction) strategy
- Development of new products or services

Responsibilities

- Statutory requirements
- Regulatory responsibilities
- Health and safety regulations

Scale

- Decide on the maximum geographic extent of a disruption or extent of resource loss that the organisation wants to, or needs to, plan to survive. This could be determined by:
 - Geographical extent (or market/customer area)
 - Regulatory or statutory requirements
 - Products, market sectors or specific customer requirements

6. Methods and Techniques

Key tools to assist:

- Outline understanding of the organisation's future plans
- Current management information outlining process details, volumes, targets and, where possible, quantified value of the activity

It is possible that some information will be market / industry sensitive and so in some organisations it will not be visible to the BCM professional. Not having this information should not stop the BIA or Risk Analysis activity being undertaken but may prejudice the accuracy of the end results.

7. Outcomes and Deliverables

- A scope and terms of reference document for the Business Impact Analysis and Risk Assessment.

8. Review

The impact of organisational strategy on business continuity management should be reviewed as a minimum annually as part of, or at least to coincide with, the business operational and strategic planning processes. More frequent review may be triggered by any of the following:

- Key business change or restructuring
- Expansion/contraction
- New product introduction
- Relocation or location consolidation
- An incident and the associated recovery

1a.2 BCM POLICY CONTENTS

Ref: BS 25999-1 Section 4.3 & BS 25999-2 Section 3.2.2

1. Introduction

The BCM Policy of an organisation provides the framework around which the BCM capability is designed and built.

2. Precursors

An organisational understanding of BCM and its importance.

3. Purpose

The purpose of a BCM Policy is to provide a documentation of the principles to which the organisation aspires and against which its performance can be audited.

4. Concepts and Assumptions

Though the senior management owns the BCM Policy, it is assumed that the BCM team will actually produce it and review it as appropriate.

5. Process

The process to develop a BCM Policy include:

- Identify and document the components of a BCM Policy
- Identify a definition of BCM
- Identify any relevant standards, regulations and legislation that must be included in the BCM Policy
- Identify any good practice guidelines or other organisation's BCM policies that could act as a benchmark
- Review and conduct a 'gap analysis' of the organisation's current BCM Policy (where appropriate) and the external benchmark policy or new BCM Policy requirements
- Develop a draft of a new or amended BCM Policy
- Review the draft BCM Policy against organisation standards for policies or similar and related policies e.g. IT security
- Circulate the draft policy for consultation
- Amend the draft BCM Policy, as appropriate, based on consultation feedback
- Agree the 'sign-off' of the BCM Policy and a strategy for its implementation by the organisation's executive/senior management
- Publish and distribute the Business Continuity Policy using an appropriate version control system and Techniques

6. Methods and Techniques

The methods, tools and techniques of developing a BCM Policy include:

- Review of organisation's current BCM Policy.
- Desktop research of external sources for guidance e.g. regulatory, legal, industry good practice, professional bodies.
- Liaison with industry and professional bodies to understand current and developing BCM

issues and drivers.

- Identification and adoption of components of a BCM Policy of another organisation that is considered Good Practice.
- A current state assessment 'gap' analysis and review of internal and external policies to derive core components of a new or amended BCM Policy
- Review by external professional BCM practitioners

7. Outcomes and Deliverables

The BCM Policy, which will include (or reference in a subsidiary document):

- The organisation's definition of BCM
- A definition of the scope of the BCM programme (see next section)
- A documented BCM Operational Framework for the management of the organisation's BCM programme including responsibilities
- A documented set of BCM Principles, guidelines and minimum standards
- An implementation and maintenance plan for the Policy.

8. Review

- Whilst all organisational policies should be reviewed on an on-going basis, a formal review of Policy is likely to be triggered by a change in the external environment in which the organisation operates. Such changes could be regulatory or market changes.

1a.3 BCM PROGRAMME SCOPE & DETERMINING CHOICES

Reference: BS 25999-1 Sections 4.4 & 6.6

1. Introduction

- One of the frequent objections raised to the implementation of Business Continuity Management is that the programme required is too extensive if applied to the whole organisation in one process.
- The British Standard allows for the scope of compliance to apply to specific products, services or one or more geographic locations. This enables an organisation to implement BCM only in some parts of the organisation initially though it is anticipated that they will wish to extend it to the whole of its operations over time
- This section spells out the choices available to the organisation to protect its delivery of products and services. Within the British Standard BS 25999-1 only the 'Business Continuity' route (section 6.6.2) can be claimed to confirm since the others (sections 6.6.3/5) - acceptance, transfer and terminate - do not imply that product and service delivery will be maintained to the customer. The choices to which this section refers are in defining the scope of the BCM programme to which the standard is then to be applied.

2. Precursors

- Logically the decision on the scope of the BCM programme is the first activity. However this is likely to be a matter of constant review and conducting a high-level BIA of product and service delivery may be a useful contribution to making a decision on which products and services to include within the scope (based on the impact of non-delivery).

3. Purpose

- The purpose of setting the scope is to ensure clarity of what areas of the organisation are included within the BCM programme. The documentation of 'Choices' for each product and service is intended to make explicit how the organisation intends to protect (or not) its ability to maintain their delivery so this decision is available for external scrutiny for example by customers or regulators.
- The scope can be (and within the standard must be) defined by identifying which products and services fall within in it. This focuses on the key success criteria of most organisations - the delivery of products or services.
- Location may also be used to define scope allowing the BCM programme to include or exclude one or more sites. However it is not logical to exclude a site which plays a part in the delivery of a product or service that is within the scope.
- The limitation of scope should be seen as a tactical approach that allows a staged development to the introduction of BCM across an organisation.

4. Concepts and Assumptions

If a product or service is identified within the scope then all activities that support its delivery must therefore be included in the BCM programme.

The BS 25999 organisation

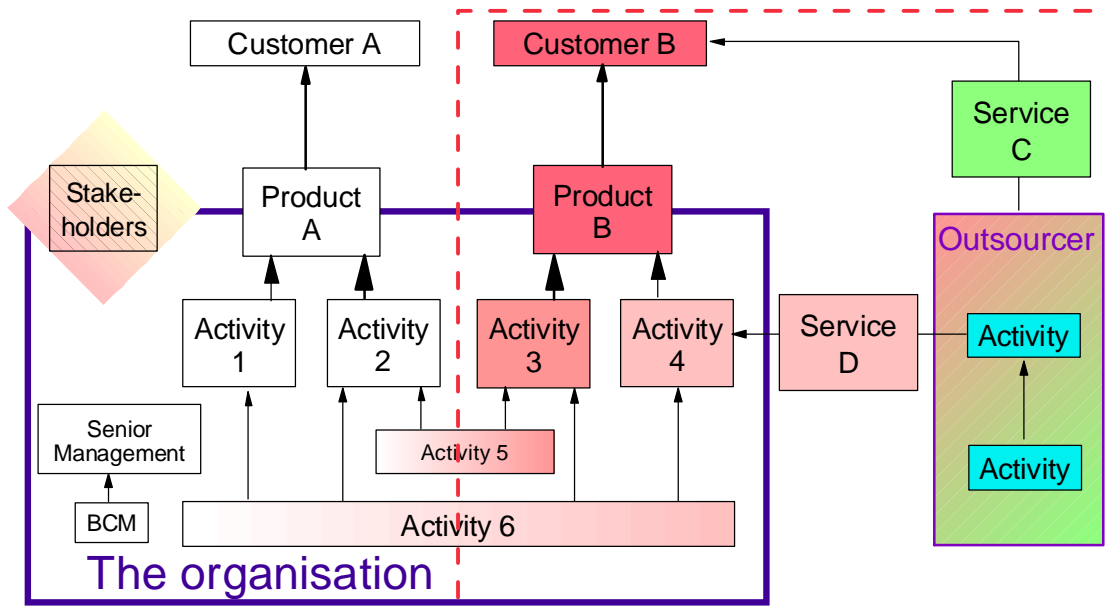


Diagram: The BS 25999 organisation

In the above diagram if it is decided that Product B and Service C are within scope of the programme then the shaded activities are necessarily fully or partly within the scope.

5. Process

The process includes the following stages:

- Form a Business Continuity Management Strategy team or group
- Identify the organisation's Business Strategy, its objectives ethical policy, legal and regulatory requirements and understand how a Continuity Strategy will support these objectives.
- If a Business Impact Analysis has been conducted to ascertain the effects of a loss of product and services review its scope, assumptions and findings
- Consider the strategy options for each product and service.
- Provide executive management with the evaluation report to choose options, which they can determine based on the organisation's current and future business strategy.
- Ensure the agreed outline option is 'signed-off' by the executive management including the financial and resource provisions.
- Implement an on-going process to ensure the strategy is reviewed.

Criteria of choice

Products and services should be identified at an appropriate level of detail.

Examples of products and services include:

- A manufactured product or range
- Waste collection (for a municipality)

- Telephone support (for a software company)

Decisions on which products, services or locations to include within the scope may be prompted by one or more of the following factors:

- A customer requirement
- A regulatory or statutory requirement
- Perceived high-risk location due to proximity to other industrial premises or physical threats such as flooding
- Product being an overwhelming proportion of organisational income

Reasons why product, service or location may be excluded from the scope:

- Product/service nearing end of life (would be terminated if supply interrupted)
- Product/service with low margins (termination or outsourced)
- A perceived low- risk location

When assessing exclusion from the scope the following factors should be considered in addition to financial impacts of loss:

- The views of all influential stakeholders
- Any reputation damage that may result from an interruption or termination of a product
- The reliability of any risk assessment

Choices

The choices available for each product and service are:

- Business Continuity
- Acceptance
- Transfer
- Change, suspend or terminate

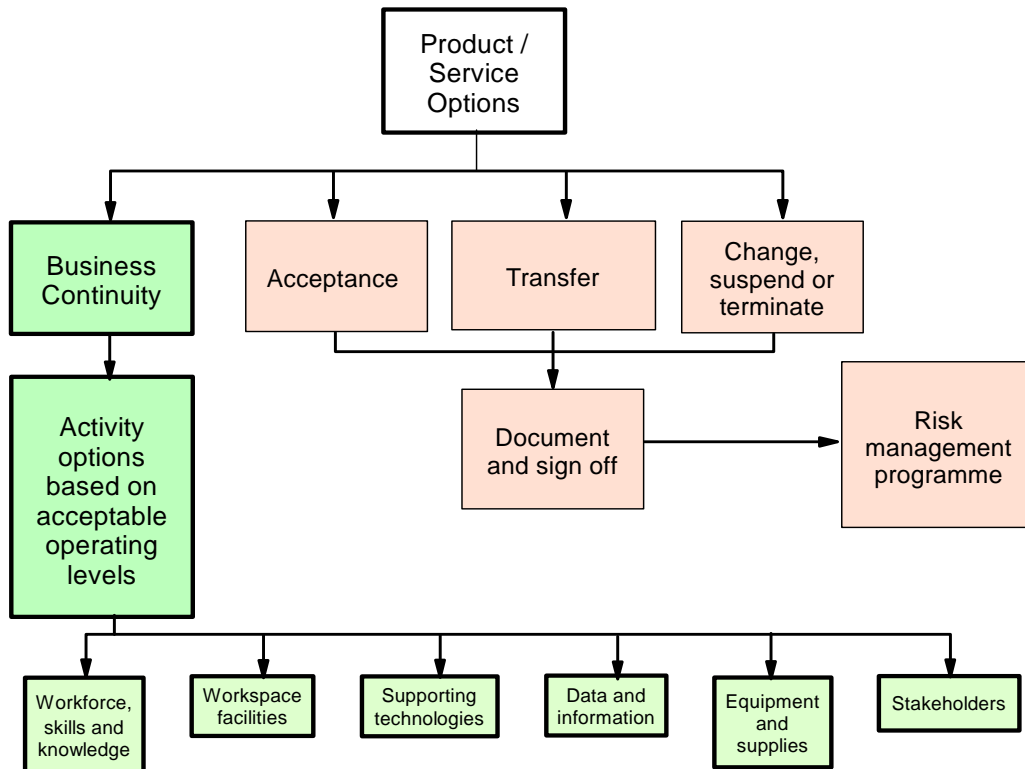


Diagram: Product and services choices

Each option is described below in more detail.

Business Continuity

If Business Continuity is the chosen strategy then it requires that suitable measures are put in place to ensure that the various activities supporting their delivery can be continued or recovered within the required timescales.

Alternative strategies to be considered (which are then outside the scope of the BCM programme) are:

Acceptance

If the cost of BCM is judged to be too high or the risk is deemed low (because disruption is felt to be unlikely or would have a low impact) then the risk can be 'accepted'.

In this event the organisation may choose to do nothing about it or put in place measures to deal with it if the risk occurs. Such measures may include:

- An Incident Management capability
- Measures to protect against specific high-probability threats such as fire
- Fortress approach- for sites with unique manufacturing process or where the location is unique then a relocation strategy may not be possible. In this case all the effort must go into minimising specific threats in the hope that, if the worst happens, the uniqueness of the organisation will require its reinstatement however long this takes.

Acceptance of a risk and determination of an organisation's 'risk appetite' is subject to all the caveats in the preceding section on evaluating threats i.e. that it is not possible to scientifically determine a value for an operational risk therefore an organisation cannot measure this accurately against its theoretical 'risk appetite'.

If an organisation seeks to protect against specific perceived threats then the overall cost of the measures may exceed that of a Business Continuity strategy and result in a less comprehensive and resilient protection than would have been provided by a BCM programme.

Transfer

A risk may be transferable to a third-party who may be more able to manage it.

Such measures include:

- **Outsourcing.** More and more organisations are outsourcing business critical processes and activities to create virtual organisations. Transfer of risk is often cited as a reason for outsourcing. It is important to remember that the risk to the organisation's reputation and brand image cannot be shifted to either intra-organisation sourcing or outsourced providers ; the risk and responsibility always remains with the business.
- **Off-shoring,** using in-house resource or outsource providers away from the centre of the business (usually in a far country), introduces additional complications in security, political and environmental risk which may attract heightened interest from customers and regulators.
- **Insurance** - transferring some of the financial costs of an incident to an insurance company. However in a major incident this can only provide money to support other business resumption measures and is not sufficient as a solution on its own.

It must be noted that some responsibilities cannot be transferred - the organisation may still suffer reputational damage or be liable to penalties as a result of the failure of the company to which they have outsourced.

Change, suspend or terminate

Changing the process may provide an opportunity to continue with the business as far as the customers are concerned, but the deliverable is 'assembled' in a different way, usually by outsourcing all or part of the operation. For example a manufacturing company may become a distributor by importing and re-badging.

Ceasing or selling parts of the business may be appropriate where the remaining business remains viable and may create space for recovery or if a product or service is nearing the end of its life span. This may also be an appropriate strategy for a Group of companies who are unwilling to budget for recovery capability in a marginal subsidiary. There are risks with this strategy if the reputation of the remaining business may be tarnished by the failure of the ceased part.

If these options are not agreed with the customer then the organisation faces the threat of possible litigation and reputation damage in the event of a failure to deliver to the customer's expectation.

However provided this strategy is agreed these options could be viewed as Business Continuity solutions and could be included within the BCM programme.

What constitutes an acceptable Business Continuity strategy may depend on the customer's acceptance of it and any change in their processes that would be necessary to accommodate it (whether determined in advance or anticipated after the event).

6. Methods and Techniques

The tools that could be used to develop the organisation's choice of strategy for products and service include:

- **Business Impact Analysis** provides a technique for systematically assessing the impact of disruptions to supply of products and services. This can be used to make a decision as to which products and services should be included within the scope of the programme

based on the timescale and extent of the impact of the disruption.

- Cost Benefit Analysis (including stakeholder, legislative and regulatory assessment)
- SWOT Analysis (Strengths/Weaknesses/Opportunities/Threats)
- Financial Planning and Management
- Strategy planning tools
- Benchmarking against appropriate national and international standards
- PEST Analysis (Political/ Environment/Social/Technical)
- Market analysis techniques may be used to determine the likely viability of a product following a disruption to supply.

7. Outcomes and Deliverables

The outcomes are:

- an agreed strategy for protection of each of the organisation's products and services which will be either within or without the scope of the BCM programme
- a scope for the BCM programme which is documented in the BCM Policy

8. Review

A review of the organisation's (Corporate) BCM Strategy should be carried out at least every 12 months. However, events may prompt re-examination of the BCM Strategy such as:

- A Business Impact Analysis revision which identifies substantive changes in processes and priorities.
- A significant change in one or more of the following: the organisation's attitude to risk (perhaps prompted by an event), market conditions, acquisition or merger, new products or services, regulatory or legislative requirements.

1a.4 OUTSOURCED ACTIVITIES

Reference: BS 25999-1 Section 4.5

1. Introduction

If part or all of a product or service delivery is outsourced, the responsibility for its continuity remains with the organisation. Customers will expect the organisation to have made an informed choice about their partners and taken appropriate measures to assure delivery. Statutory and regulatory requirements usually emphasise that ultimate responsibility for outsourced services remains with the organisation.

2. Purpose

The purpose is to ensure that the organisation's delivery of products and services is not disrupted by a failure of a third party supplier of goods or services which are provided either to the organisation or direct to the customer on the organisation's behalf.

3. Concepts and Assumptions

The responsibility for delivery of the product or service remains with the organisation and cannot be transferred to the outsourcing company.

4. Process

The processes for reviewing the Business Continuity arrangements of an outsourcing company are similar to those employed for reviewing the organisation's own arrangements (see later *Section 5*).

It is important that access to this information is available for assessing:

- tenders of prospective outsourcers
- on-going adequacy of arrangements of existing outsourcing companies

5. Methods and Techniques

Resilience in outsourcing arrangements may be increased by:

- Appropriate selection of outsourcing companies
- Specification of BCM requirements in contract terms
- Agreement on realistic Service Levels for use during incidents at either organisation
- Involving outsourcing companies in BCM training, awareness and exercising

6. Outcomes and Deliverables

Documentation to support outsourcing include:

- Mandatory parameters for selection of outsourcing companies
- Contract terms
- Service Level Agreements
- Documentation of results of exercises

The outcome should be a resilient supply chain which can manage disruptions without seriously impacting the delivery of products and services to the customer.

7. Review

The review of supplier continuity should form a significant part of the assessment of tenders when contracts are being awarded or renewed.

Annual review of supplier performance against continuity requirements is recommended.

1b. PROGRAMME MANAGEMENT

Reference: BS 25999-1 Section 5

1. Introduction

A key success factor of the BCM is the appointment of competent persons to oversee and manage the BCM programme.

Whilst initially BCM may benefit from a project management approach, as BCM matures within an organization, programme management skills are required to ensure a preparedness remains current.

Key steps in BCM Programme Management are:

- Assigning responsibilities
- Implementing BCM in the organisation
- Project Management
- Ongoing management
- BCM documentation
- Incident readiness and response

1b.1 ASSIGNING RESPONSIBILITIES

Reference: BS 25999-1 Section 5.2 & BS 25999-2 Section 3.2.3/4

1. Introduction

The key to a successful BCM programme is the early identification of clearly defined roles, responsibilities and authorities to manage the BCM programme and process throughout the organisation and the continued readiness of the appropriate personnel to respond when required.

2. Precursors

The BCM Policy should identify the roles and responsibilities required to be assigned.

3. Purpose

The purpose of assigning roles and responsibilities is to ensure that the tasks required to implement and maintain the programme are allocated to specific, competent individuals whose performance can be monitored.

4. Concepts and Assumptions

Regulatory Authorities such as the UK Financial Services Authority (FSA) consider that BCM is a cost of doing business and needs to be adequately resourced.

5. Process

A member of the Executive should be given overall accountability for the organisation's BCM capability and its effectiveness. This ensures that a BCM programme is given the correct level of importance within the organisation and a greater chance of effective implementation.

An individual should be appointed to manage the BCM programme. This person may be known as the BC Manager.

Depending on the size of the organisation, additional staff may be nominated to work with the BC Manager these may be:

- BCM staff to assist with the BCM role - to conduct exercises and information collection
- BCM administrative staff who undertake documentation revisions
- Staff in other business units or locations who assist in BCM implementation and act as BCM coordinator in their areas.

Additional groups may be formed to assist in the development of the BCM programme such as:

- BCM Programme Board - a management group to give advice, guidance and management oversight
- BCM Team - the operational team that would respond in an incident who should contribute significantly to writing of the BC plan
- Incident Response Forum - a forum comprising representatives of all teams involved in incident response to resolve coordination issues. This group may be a useful focus for identifying training and exercising requirements.

6. Methods and Techniques

The Staff appointed to the BCM programme should have the appropriate training for their role using in-house or external training courses.

Those managing the programme should seek a level of certification from an appropriate professional body such as the Business Continuity Institute.

The integration of roles and responsibilities into job descriptions and the appraisal process may be effective in ensuring that these tasks are given appropriate time and effort. Successful completion should be reflected in the organisation's reward and recognition policy. Remove?

7. Outcomes and Deliverables

The roles and responsibilities of individuals within the BCM programme will be included in job specifications and performance objectives.

Roles and responsibilities will be understood by individuals and the organisation.

8. Review

The level of BCM staffing should be a topic for the BC Manager's annual appraisal and may be the subject of an audit.

1b.2 IMPLEMENTING BCM IN THE ORGANISATION

Reference: BS 25999-1 Section 5.3

1. Introduction

Initiating a BCM Programme involves the coordination of a number of activities that balance:

- Awareness-raising events which maintain the enthusiasm for undertaking a BCM programme
- Activities of data collection that will educate the choice of continuity options to support organisation's objectives
- Implementation of measures to mitigate the impact of an incident should it occur as the programme is being developed.

2. Precursors

A BCM Policy within which the programme can be defined and properly budgeted staff resources.

3. Purpose

The purpose of this step is to ensure that a sustainable BCM programme is implemented in the organisation. A sustainable programme is one that has gained the commitment of the organisation and has structures and procedures in place to ensure that readiness is maintained and enhanced for the foreseeable future.

4. Concepts and Assumptions

The choice of which activities to undertake and in what order will depend on the existing culture and state of readiness of the organisation. The only definite rule is that major decisions on continuity options and recovery strategy should not be made until the 'Understanding the Organisation' stage has been undertaken.

External assistance from consultants with appropriate BCM qualifications and experience may be used to initiate a BCM programme. This can be cost-effective in saving development time and the need for external training. Knowledge transfer to in-house staff should be an objective during this period.

5. Process

The initiation process should be constructed from activities described elsewhere in this document. These could include:

- Awareness raising activities:
 - A desktop exercise with senior managers to demonstrate what would happen in the absence of an incident response structure and procedures
 - Presentations on the impact of recent local incidents
 - Questionnaires or interviews to determine the current state of readiness within the organisation
 - Drafting a scope for the programme
 - Discussion to draft a BCM Policy
- Data collection and continuity option selection:
 - Training programme for team to undertake Business Impact Analysis (BIA)
 - Awareness programme for managers to improve understanding of BCM and improve

response to BIA questions

- BIA and Recovery Requirements Analysis
- Workshops to analyse results
- Workshops with senior management to choose continuity options
- Measures to mitigate specific perceived threats
- Create incident management procedures
- Identify and implement low cost quick wins

6. Methods and Techniques

The methods, tools and techniques to develop a BCM Programme are described in this document. A Project Management method should be used to monitor progress.

- When used during a programme initiation, sufficient time should be allowed to support each activity with appropriate awareness and skills training

7. Outcomes and Deliverables

At the end of a successful initiation of a BCM Programme the organisation should have:

- A satisfactory state of readiness - often demonstrated by a desktop exercise of the incident management procedures
- Procedures, structures and skills to maintain and develop the BCM capability

8. Review

The BCM programme whilst in an initiation phase should be reviewed at least monthly and on completion of defined milestones.

1b.3 PROJECT MANAGEMENT

Reference: BS 25999-1 Section 5.3.2

1. Introduction

When implementing a BCM programme for the first time in an organisation, project management disciplines should be adopted.

This gives way to on-going programme management once the key elements are in place. However this remains a useful discipline for elements of an on-going programme that have a clear deliverable for example in rolling out an awareness event across the organisation.

2. Precursors

Selection of an accepted Project Management method.

3. Purpose

To generate an initial impetus for BCM implementation the disciplines of a project management method may usefully be employed such as:

- Identification of deliverables
- Timescales and deadlines
- Budget and work effort control

4. Concepts and Assumptions

Whilst a clear deliverable can be identified for some BCM tasks many others are less tangible making strict project management disciplines difficult to implement. For example there is often an element of 'discovery' within a BIA making it difficult to quantify the time required to complete it.

5. Process

This document can be used to define a project plan for the initial implementation of a BCM programme. Typical project stages with defined deliverables are:

- Awareness raising - making the case for BCM
- Defining programme scope (Write Policy)
- Business impact analysis
- Risk Analysis
- Continuity option selection
- Developing and implementing the response
- Developing and managing a desktop exercise to test the first draft of a plan

Work estimates for some project stages will often depend on the outcomes of previous stages. A project method may also be usefully applied to individual items with a clear deliverable within the BCM programme such as:

- Developing and managing a BCM exercise
- Developing and delivering a training programme to staff
- Selecting a supplier for a continuity resource

6. Methods and Techniques

There are several project management methods, many with software support. An appropriate method should be used for the size and complexity of the organisation.

7. Outcomes and Deliverables

The initial implementation of the BCM programme may be undertaken by a series of projects with clear deliverables and work estimates.

8. Review

The project method adopted should include the requirement for regular review of progress against pre-defined dates for milestones and work estimates.

1b.4 ONGOING BUSINESS CONTINUITY MANAGEMENT

Reference: BS 25999-1 Section 5.4

1. Introduction

An effective BCM programme will involve the participation of various managerial, operational, administrative and technical disciplines that need to be co-ordinated throughout its lifecycle using procedures such as those outlined in these guidelines.

The programme should be managed within the framework and according to the principles contained in the organisation's BCM Policy document.

2. Precursors

Successful implementation of the programme initiation activities.

3. Purpose

The purpose of the management process is to provide the effective ongoing management of the organisation's BCM programme.

4. Concepts and Assumptions

The number of professional BCM practitioners and staff from other management disciplines that may be required to support and manage the programme depends upon the size, nature, complexity and geographical location of the organisation.

In smaller organisations the BCM activity may be given to an individual along with other roles. In a larger organisation there may be several staff with full-time or part-time BCM responsibilities. In this case a hierarchy may be established and staff management skills (in addition to BCM skills) may be required by those managing the programme.

5. Process

The Executive of the organisation should:

- Appoint a person or team to manage the BCM programme
- Define the scope of the management process and programme
- Approve the continuity budget
- Monitor the performance of the management process

The appointed BCM team should (in consultation with the executive):

- Develop and approve a BCM planning process and programme.
- Determine the key approaches to each stage of the BCM lifecycle as described below
- Undertake or manage the appropriate BCM activities within the organisation
- Promote BCM across the organisation and externally where appropriate
- Manage the continuity budget
- Maintain the BCM programme documentation
- Research the current state of readiness of organisations in the same sector and the level required by legislation and regulation
- Report on the current state of readiness to the Executive on a regular basis highlighting where there are identified gaps

The BCM team may (in consultation with business managers) identify and train BCM representatives in operational departments or at other locations to:

- Act as a point of contact for BCM issues affecting the department or location
- Assist the department to identify the BCM implications of process change
- Notify the BCM team of process changes
- Assist or lead the department's or location's recovery in the event of a disruption.

6. Methods and Techniques

The methods, tools and techniques to manage an organisation's BCM programme may include:

- BCI Good Practice Guidelines
- A BCM self assessment scorecard
- Annual Personal Performance Contracts and Appraisals
- Supplier and outsource provider relationship management of business products and services
- Supplier relationship management of BCM specialist resources and services
- Financial management
- Legal and regulatory advice
- Industry BCM Benchmarking
- National and International Standards such as the BS 25999
- Internal and/or independent BCM audits
- Review and challenge

7. Outcomes and Deliverables

The deliverables of the BCM programme include:

- A clearly defined and documented BCM programme that is agreed by the organisation's executive/senior management.
- BCM assurance reports at a predetermined frequency
- Clearly defined and documented BCM Strategy and Standards
- A management process that is an integral part of the organisation's BCM programme and life cycle
- The overview and provision of the organisation's recovery solutions.
- The BCM programme annual budget bid
- The BCM programme audit report
- The provision and maintenance of an effective BCM competence and capability
- Successful notification, escalation, invocation and recovery experiences

8. Review

An organisation's BCM programme should be managed on an ongoing basis.

The programme should be reviewed by internal or external audit on a timescale that they define.

1b.5 DOCUMENTATION

Reference: BS 25999-1 Section 5.5 & BS 25999-2 Section 3.4

1. Introduction

An important part of the BCM process is to manage all BCM documentation. This needs to be carried out in a manner that is consistent, easy to understand and provides both operational and audit/review support. The level and type of documentation should be appropriate to the type and size of the organisation.

2. Precursors

Organisations that are certified against other management standards such as ISO 9000 or ISO 27001 will need to review how BCM documentation fits with the requirement of those standards.

3. Purpose

The BCM documentation has three purposes:

- To manage the programme effectively
- To prove the effective management of the programme during an audit
- During a disruption - to have current and effective documentation available that may be required for incident management and resumption

4. Concepts and Assumptions

Although it is important to maintain BCM documentation, its presence on its own is not proof of a capability to respond to an incident.

Adequate training must be given to staff in the operation of any software used in the programme. Those responsible for maintaining plans should be able to update their documentation since this promotes ownership and reduces the clerical overhead of central BCM administration.

Specialist BCM software may offer some advantages in maintenance but imposes an ongoing cost of training throughout the programme.

5. Process

The maintenance of BCM documentation should be integrated into the organisation's change management procedures.

6. Methods and Techniques

Software can be used to manage the BCM documentation.

- Word processing software can be used for text documents such as the Policy
- Spreadsheets, flowcharting tools, project management software and databases can be used for the logistics of response plans
- Specialist software can be used for plans
- Software can also be used to ensure current copies of documents are available at the organisation's various sites

A document control system should be established to manage:

- Usability and accessibility
- Approval

- Update and review
- Version control
- Distribution control
- Archiving or destruction of obsolete documents

7. Outcomes and Deliverables

A current set of BCM documentation. This may include:

- BCM Policy including scope and principles
- BCM roles, responsibilities and resources
- Training and competency records for BCM personnel
- Business Impact Analysis
- Risk analysis
- BCM Strategies including papers supporting the choice of the strategies adopted
- Response plans
 - Incident Response structure
 - Incident Management Plans
 - Business Continuity Plans
 - Departmental Business Resumption Plans
- Exercise Schedule and reports
- Awareness and training programme
- Service Level Agreements with customers and suppliers
- Contracts for third party recovery services such as workspace and salvage
- A Maintenance and review (audit) programme, reports and corrective actions

8. Review

The review cycle for each document is identified in the sections that relate to its creation and use.

The documentation and controls should be reviewed by internal or external audit on a timescale that they define.

1b.6 INCIDENT READINESS & RESPONSE

1. Introduction

Those involved in Business Continuity may be expected to provide a lead during incident response.

2. Precursors

BCM professionals should maintain a state of readiness so that incident management takes over smoothly if called to put plans into action.

3. Purpose

The BCM Team have best detailed knowledge of the overall strategies and actions that need to be immediately invoked. They will need to support line management with assessment and invocation activities until the Incident Management Team is fully operational.

4. Concepts and Assumptions

It is often assumed that those who have developed the plan are the best individuals to respond to an incident but the personality characteristics required of planners and leaders are often contradictory. Any difficulties in this area should be exposed by a realistic set of plan exercises.

5. Process

Receive notification of problem.

Assess situation then:

- either manage response through appropriate prepared plans
- or escalate to Incident management team

If a response is required then immediate things to consider include:

- are you physically and emotionally fit to assist or lead a response
- are the others from whom a response is required present and able to undertake the roles assigned to them - some people may react to an incident with unusual behaviour
- have you communicated what has happened to senior management

6. Methods and Techniques

There are many incident management methods; a generic one is suggested here.

- Contain - Is there anything that can be done immediately to stop the problem getting worse?
- Look at the Plan - is there a pre-planned response that fits this incident?
- Follow the documented procedure which may include the following steps:
 - communicate - trying to solve the problem on your own may waste time if the situation then gets out of control.
 - if necessary assemble a team to respond to the incident
 - assess the situation - Find out as much as you can without putting yourselves at risk
- Predict the likely outcome - and adapt the BC Plan to provide a response strategy
- Predict a 'worst case' outcome - and have a 'back-up' response strategy
- Escalate the response to the required level within the organisation

- Implement the response strategy
- Evaluate the progress of the response against the likely outcome
- As soon as the situation allows, review the effectiveness of the response

7. Outcomes and Deliverables

The outcome of a successful response is a controlled return of the organisation to business as usual.

8. Review

As soon as possible after the interruption the organisation's response should be evaluated and any necessary changes made to procedures, personnel or contracts.

END OF SECTION 1 - BCM Policy and Programme Management