



**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

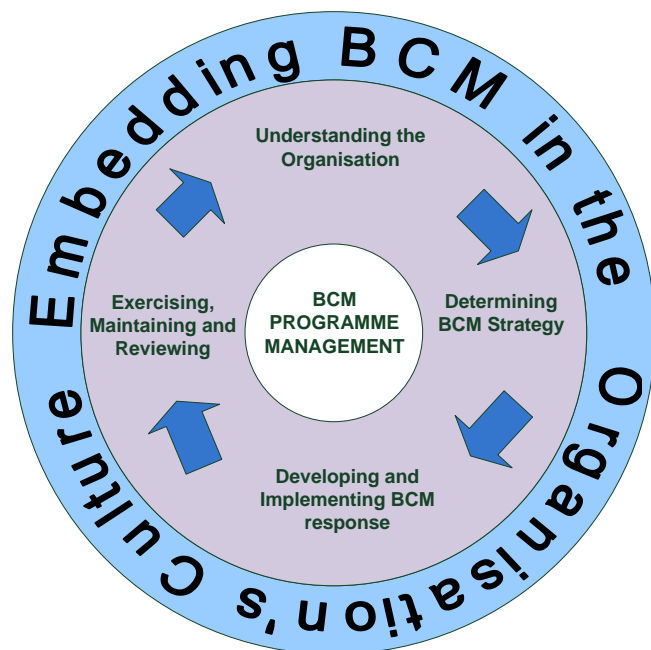
The structure and format of each component follows a common pattern:

<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

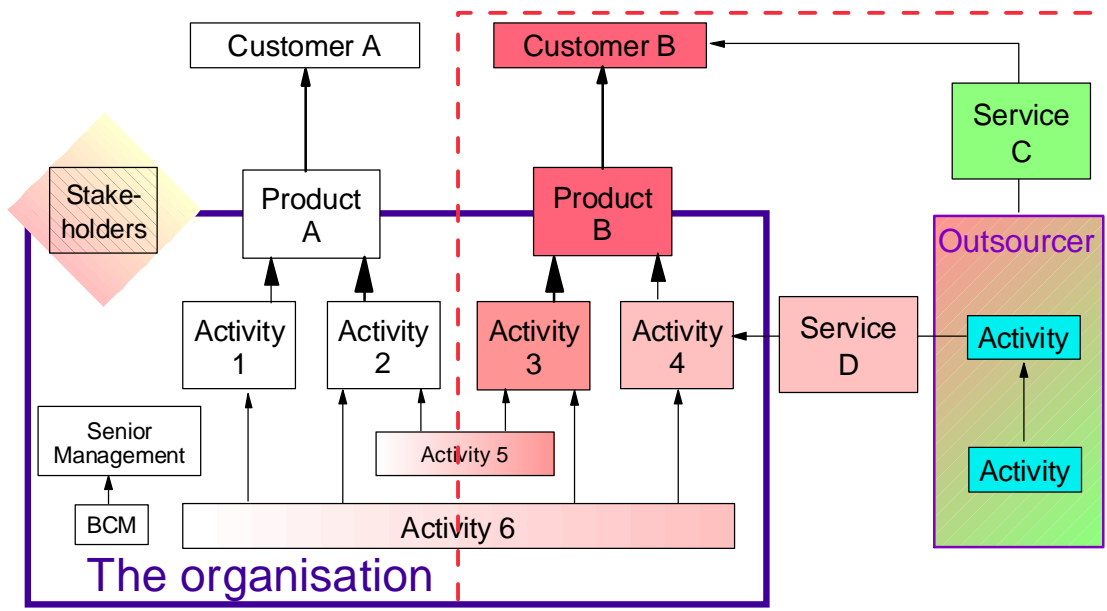


Diagram: The BS 25999 organisation

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

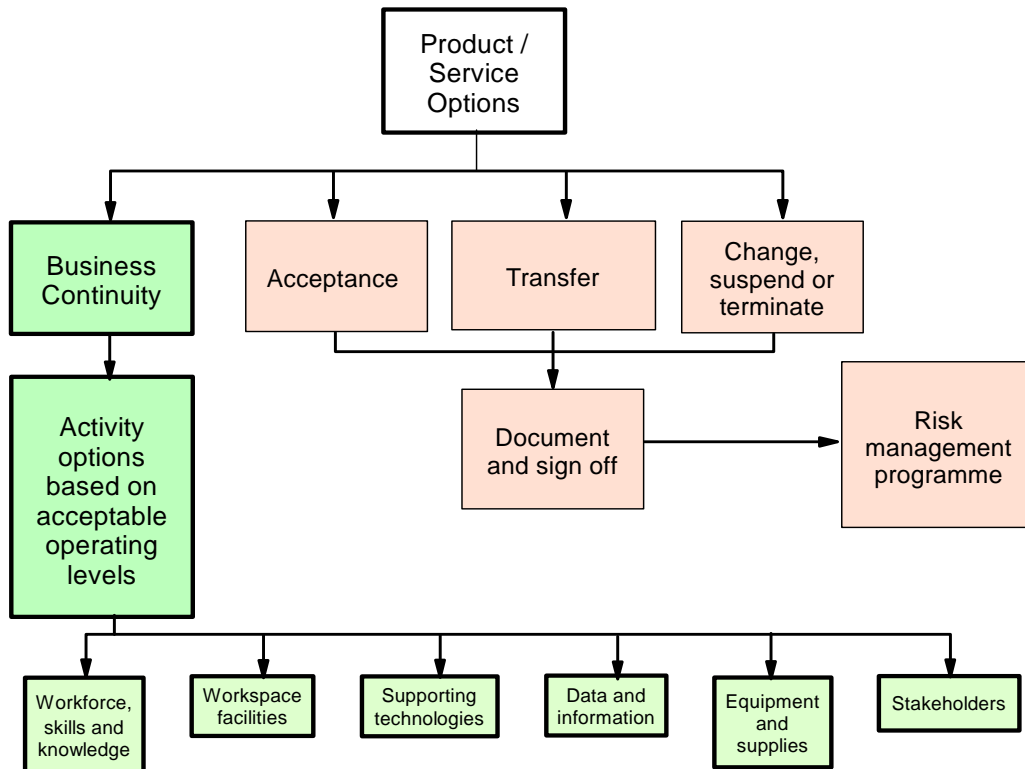


Diagram: Product and services choices

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



**BUSINESS CONTINUITY
INSTITUTE**

**GOOD PRACTICE GUIDELINES
2008**

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

**SECTION 2
UNDERSTANDING THE
ORGANISATION**

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. 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**

At the end of each section there is a summary of "Key BCM Indicators" that will support future use of the BCI Benchmarking Tool, BCI E-Learning and BCI Entrance Examinations.

The view presented in these Guidelines attempts to provide 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.

Before referencing this Section of the Guide, you are advised to read Section 1, which explains in more detail how the guide works and how to use it most effectively.

3. About Section 2 - Understanding The Organisation

Business Continuity Management 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.

Understanding the Organisation is a key element of good Business Continuity Management. It seeks to identify the key products and services of an organisation, and consequently define the time-criticality of activities that support them. This part of the BCM must be fully integrated

into the organisation's objectives, obligations and statutory duties.

A thorough understanding of the business through Business Impact Analysis (BIA) and Risk Assessment (RA) in combination can often highlight business inefficiencies and focus on priorities that would not otherwise be apparent to senior management.

GUIDELINES STAGE 2: UNDERSTANDING THE ORGANISATION

COMPONENTS

2.0 UNDERSTANDING THE ORGANISATION	4
2.1 BUSINESS IMPACT ANALYSIS	5
2.2 ESTIMATING CONTINUITY REQUIREMENTS	10
2.3 EVALUATING THREATS (RISK ASSESSMENT)	12

2.0 UNDERSTANDING THE ORGANISATION

Reference: BS 25999-1 Section 6

1. General Principles

As described in the section on BCM Policy, the organisation must make a clear decision on whether the BCM will cover the whole organisation or just certain products or services. This sets the scope of the Business Impact Analysis (BIA) and Risk Assessment (RA) steps.

The tools for understanding your business for business continuity purposes are:

- Business Impact Analysis (BIA) - a mandatory process for evaluating the impact over time of a disruption to an organisation's ability to operate
- Continuity Recovery Requirements analysis - to estimate the resources, facilities and external services that each activity will require at resumption
- Risk Assessment(RA) - to estimate the likelihood and impact on specific functions from known threats

The BIA identifies the urgency of each business activity undertaken by the organisation by assessing the impact over time of an interruption to this activity on the delivery of products and services. This information is used to identify the timescale of appropriate continuity and resumption strategies for each activity individually and in relation to one another.

The Continuity Requirements Analysis provides the information that will allow the scale (size and numbers) of the appropriate continuity measures to be determined.

Risk Assessment (RA) activity helps in identifying potential causes of interruption to an organisation, the probability of occurrence and impact of the threat being realised. Measures can then be identified that attempt to reduce the probability of occurrence or reduce the impact of an incident arising from these specific threats. Within the BCM programme, a RA should focus on the specific technologies and inherent risks of the business activities identified as most urgent in the BIA results rather than on all risks to the organisation.

2.1 BUSINESS IMPACT ANALYSIS

Reference: BS 25999-1 Section 6.2–3 & BS 25999-2 Section 4.1.1

1. Introduction

The Business Impact Analysis (BIA) is the foundation work from which the whole BCM process is built. It identifies, quantifies and qualifies the business impacts of a loss, interruption or disruption of business processes on an organisation and provides the data from which appropriate continuity strategies can be determined.

A Business Impact Analysis can be used to identify the timescale and extent of the impact of a disruption at several levels in an organisation. For example to examine the effect of:

- The loss of the ability to deliver each product or service - to educate decisions on the scope of the BCM programme
- An interruption to the internal and external activities that that would disrupt the delivery of products and services - to provide the information for selection of continuity options and their resource requirements
- A disruption of a business area's activity - to assist the preparation of a detailed plan for the department

Once the scope is determined the BIA focuses on the activities (which support those products and services) identifying those whose failure would most quickly threaten delivery. These tend to be the 'operational' activities, which interact directly with customers or other outside organisations. However these activities may depend for their delivery on the 'support' of other internal and external process, which must also be analysed.

- Examples of operational functions include:
 - Customer service
 - Sales
 - Production
- Examples of support functions include:
 - IT
 - Human resources
 - External support services such as utilities
- Examples of strategic activities include:
 - Management
 - Projects
 - Planning

2. Precursors

It is necessary to obtain the full support of the Executive or most Senior Management Group before a Business Impact Analysis is attempted. It is unlikely that managers will be prepared to dedicate time to this exercise unless this top tier support is demonstrated.

A decision about which products and services are within the scope of the BCM programme may have been made before a BIA is undertaken which will be documented within the Business Continuity Management (BCM) Policy. Alternatively the BIA method can be used to understand the impact of the failure to deliver the product or service. This can then be used to educate this decision.

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 implements the required capabilities. To be able to develop an appropriate Business Continuity Management programme you must ensure that it reflects organisational objectives and culture (See Section 1a)

3. Purpose

The purpose of a Business Impact Analysis is - for each activity or product and service:

- To document the impacts over time that would result from its loss or disruption.
- Identify the Maximum Tolerable Period of Disruption (MTPD)
- Identify the dependencies (both internally and externally) that are required to enable the activity to operate effectively

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

4. Concepts and Assumptions

Concepts

- Maximum Tolerable Period of Disruption (MTPD) - this is the duration after which an organization's viability (either financially or through loss of reputation) will be irrevocably threatened if delivery of a particular product and service cannot be resumed.
- Seasonality may affect the MTPD. As examples, a financial year-end may reduce the tolerable outage for the finance activity and a one-off contract with significant time penalties may reduce the tolerable outage for a range of functions within the organisation.
- Recovery Point Objective (RPO) - is the point to which information must be restored to enable an activity to operate once it is resumed.

Terminology 'Critical' activities

- Having ascertained the MTPD for each activity it is often convenient to link activities with similar recovery requirements. Sometimes organisations call these groups according to the recovery timescale (e.g. 1 day, 2 day, 1 week etc); others use the term 'critical' (or 'mission critical' activities) for those activities required within the first few days. Unfortunately for those unfamiliar with BCM terminology, 'critical' is often interpreted as 'important' leading to misunderstandings when collecting data for the BIA and the, incorrect, assumption that recovery tactics and plans are not required for 'non-critical' activities. Terms with less ambiguous, time related meanings in general use include 'time-critical', 'time sensitive' and 'urgent'.

Assumptions

- It is assumed that the organisation can be understood by analysis of separate business activities
- The MTPD may be difficult to determine for seasonal or periodic functions such as year-end processing and projects. In such instances impact analysis should focus on an interruption to the activity during one of these peaks
- Where resilience measures are already in place these should be assumed to be in operation (though they may prove not to be adequate)

Sensitivity of information

- 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 activity being undertaken but may prejudice the accuracy of the end

results.

5. Process

Scope and Scale

- If the organisation is part of a group - identify the relationship between the various parts of the organisation since this may affect the MTPD
- If the organisation has multiple locations identify the geographical scope of the BIA from the Policy.
- Sign off the terms of reference with the project sponsor drawn from Executive or Senior Management Group

Business Impact Analysis

- Identify business activities across the organisation (which may cut across several departments) and management owners of these processes
- Identify suitable staff from whom information can be sought about the business processes - subject matter experts
- Identify the impacts which may result in damage to the organisation's reputation, assets or financial position
- Quantify the timescale within which the interruption of each business activity becomes unacceptable to the organisation
- Where an organisation has multiple sites it may be necessary to 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 to quantify impact. This could be determined by:
 - Geographical extent (or market/customer area)
 - Regulatory or statutory requirements
 - Products, market sectors or specific customer requirements

Reporting

- Obtain sign-off by the process owner to confirm accuracy of information
- Obtain support of the BCM sponsor for the conclusions.

6. Methods and Techniques

Data collection

Methods, tools and techniques to carry out Business Impact Analyses include:

- Workshops
- Questionnaire(s) - paper and/or automated software
- Interviews (structured and unstructured)

As a general guideline:

- Workshops can provide rapid results and an opportunity for hands-on engagement with the programme provided there is consistent buy-in from all departments and participants
- Questionnaires provide large amounts of data but information quality can be very questionable if not completed with consistency
- Interviews can provide very good information but are time consuming and output can vary in format and detail

Combinations of the above methods can provide excellent results providing an appropriate level of detail and a standard reporting format that will assist in consistency of recording and

analysing information across multiple functions.

Data Collection Questionnaires

There is no 'one size fits all' methodology for BIA data collection. Methods vary from one industry sector to another and from one practitioner to another. Each industry has its own specific needs in result content, information types, depth and coverage. However a few basic principles that should be considered are:

- The objective of the BIA is to collect information to assist in the choice of appropriate continuity strategies which is determined by the urgency with which each activity needs to be resumed
- How the information collected will be used
- What is the best format of data collection to report results effectively?
- What basic information is needed to establish the urgency of the performance of the activity being analysed in isolation and as part of the organisation as a whole:
 - Timeframes within which the activity must be resumed
 - Locations from which activity is undertaken
 - Influences on the activity, e.g. peak periods, regulatory reporting
 - What is the impact of not continuing the activity
 - How long can the organisation last without it
 - Are there any alternatives?

Factors to consider include:

- Volumes, e.g. calls per hour, output on production line
- Contractual, regulatory or legal requirements
- Key tools to achieving continuity of the activity (how many, where and when):
 - People - skill set
 - Equipment - IT, telecommunications, manufacturing / industrial plant
 - Data - paper and electronic
 - Dependencies - internal and external to organisation

Software

There are a variety of proprietary software products available to conduct Business Impact Analyses that may be useful but are not essential. The key benefits of utilising a software tool include ease of analysing results, storage of information and potentially reporting of the results their use does not however remove the need for interviews with or involvement of individuals knowledgeable in the activity being analysed.

Reporting

Every organisation has its own preferred style of reporting and in some instances the reporting style may need to be adjusted to accommodate multiple audience groups within the one organisation and may include tables, graphs and charts. The organisations preferred reporting format should be established and agreed at the time of setting the scope of activity as requirements for the final report format may impact the way you choose to collect, aggregate analyse and present information.

7. Outcomes and Deliverables

The outcomes from a Business Impact Analysis are:

- The Maximum Tolerable Period of Disruption and its justification (nature of impacts) for each activity
- Recovery Point Objective (RPO) to which information used by this activity must be restored to enable an activity to operate once it is resumed.

8. Review

Good practice indicates that a Business Impact Analysis should be reviewed as a minimum annually but more frequently in the event of:

- A particularly aggressive pace of business change
- Significant change in the internal business processes, location or technology
- Significant change in the external business environment - such as market or regulatory change

This does not necessarily require the BIA to be completely redone. Careful design of the BIA report can facilitate this process by providing a benchmark against which changes in the above areas can be measured and their changed impact assessed.

2.2 ESTIMATING CONTINUITY REQUIREMENTS

Reference: BS 25999-1 Section 6.4

1. Introduction

The Continuity Requirements Analysis collects information on the numbers of resources required to resume and continue the business activities at a level required to satisfy the organisation's obligations.

2. Precursors

This step is usually undertaken at the same time as the BIA information is being gathered.

3. Purpose

Its purpose is to:

- Provide the resource information from which an appropriate recovery strategy can be determined / recommended
- Identify resource requirements resulting from activity dependencies that exist both internally and externally

4. Concepts and Assumptions

Continuity Requirements

It is often assumed that the required resources after a disruption will be a fraction of the numbers used during normal operations - at least for a period of time. However in some cases the resources in the early stages of recovery may need to be higher than normally used to cope with backlogs. For example in a call-centre additional staff may be needed to cope with the extra calls following an interruption and supporting IT systems may need to have a higher capacity to cope with this additional number of users.

5. Process

Continuity Requirements

- Quantify the resources (e.g. people, technology, telephony,) required over time to maintain the business functions at an acceptable level and within the maximum tolerable period of disruption For a period after the interruption this may be less or more than the usual resource requirement. It should take into account any extra activity that will be generated by the interruption and the need to clear backlogs.

Reporting

- Obtain sign-off by the process owner to confirm accuracy of information
- Obtain support of the BCM sponsor for the conclusions.
- Present to the Senior Management Group or Executive to determine whether results will be impacted by any proposed business change and for approval to move to strategy design stages.
- Proceed to development of BCM strategy.

6. Methods and Techniques

Data collection

Methods, tools and techniques to carry out Continuity Requirements Analyses include:

- Workshops
- Questionnaire (s) - paper and / or automated software
- Interviews (structured and unstructured) The information is usually collected at the same time as the BIA information.

7. Outcomes and Deliverables

The outcomes from a Continuity Requirements Analysis are:

- The resources required during the time after a resumption to provide agreed service levels
- Interdependencies between internal activities and on external suppliers

This information feeds directly into the Business Continuity Strategy stage. The resource requirements will provide the data to evaluate alternative recovery solutions for adequacy of size and performance.

8. Review

The Continuity Requirements Analysis should be reviewed along with the BIA.

2.3 EVALUATING THREATS (RISK ASSESSMENT)

Reference: BS 25999-1 Section 6.5 & BS25999-2 Section 4.1.2/3

1. Introduction

In the context of BCM, a Risk Assessment looks at the probability and impact of a variety of specific threats that could cause a business interruption. By prioritisation it may be possible to implement measures to reduce the likelihood or mitigate the impact of these threats.

When evaluating threats to business activities, the BIA provides an extra dimension (time) into the usual Threat Impact x Likelihood equation. It suggests that effort on implementing risk treatment measures should be targeted on those activities that will most quickly disrupt the business.

It is difficult to scope a Risk Analysis across an entire organisation however, by focusing on the resources required to operate the organisation's most urgent activities (i.e. following a BIA), the focus of the Risk Assessment can be reduced to a more manageable scope.

It should be recognised that Risk Assessment has serious shortcoming in evaluating catastrophic operational risks because:

- It is impossible to identify all threats
- Estimates of probability are guesswork or based on historic and sometimes inaccurate information.
- Impacts are not fixed ('high, medium and low') but increase over time at different rates
- The numeric scales used often over-emphasize the impact of minor events

The Risk Assessment may identify unacceptable concentrations of risk and what are known as 'single points of failure'. These should be highlighted to the business continuity sponsor at Executive or Senior Management level at the earliest possible opportunity along with options for addressing the issue. The strategic decision to mitigate, transfer or accept the risk should be formally documented and signed off.

In some countries and sectors the use of Risk Assessment is mandated.

2. Precursors

A Business Impact Analysis should be completed in advance of a Risk Assessment to identify the urgent functions upon which the risk assessment should be focused.

3. Purpose

The Purpose of a Risk Assessment is to:

- Identify the internal and external threats that could cause a disruption and assess their probability and impact
- To prioritise the threats according to an agreed formula
- To inform a risk management control programme and action plan.

4. Concepts and Assumptions

Concepts:

Whatever the complexity of the actual formula adopted the following relationship is assumed:

- Risk = Threat impact x Probability

Some risk models then order risks by: Priority = Risk x Ability to control that risk. This formula prioritises the threats that are easiest to control with, presumably, the argument that this will

give the best return on investment of time and money but at the penalty of ignoring many significant external impacts.

In other risk models the risks assessed are examined with no controls in place and then again with current and desired controls in place. This second step serves to emphasise that assumptions when managing the risk control environment should not be made and that the effectiveness of controls should always be examined and as applicable, challenged and improved. If an organisation decides after taking this second step that they do not wish to improve controls - perhaps due to prohibitive cost - then the Risk and BCM managers need to be aware of this and factor this decision into their approach.

The organisation's 'risk appetite' or 'risk tolerance' is the amount of risk that an organisation is prepared to accept and drives the level of action it will take to control identified threats.

Assumptions

- All realistic threats can be identified
- Accurate and applicable statistics are available to estimate the probability of occurrence
- Threats which are easier to control (staff or own building issues) are to be prioritised at the expense of those which are less susceptible to influence - such as bad weather
- The use of a numerical scale to assign a value to impacts can adequately reflect the relative importance of less-quantifiable assets such as reputation
- The use of a numerical scale (1,2,3..) represents a realistic relationship between the different impact and probability bands (where in reality a logarithmic scale may be more realistic (e.g. 1, 10, 100, 1000...))

5. Process

The key stages in a Risk Assessment are:

- Tabulate a scoring system for impacts and probabilities and agree with project sponsor
- List threats to the urgent business processes determined in the BIA.
- Estimate the impact on the organisation of the threat using a numerical scoring system
- Determine the likelihood (probability or frequency) of each threat occurring and weight according to a numerical scoring system
- Calculate a risk by combining the scores for impact and probability of each threat according to an agreed formula
- Optionally prioritise the risks according to a formula which includes a measure of the ability to control that threat
- Obtain organisation sponsor's approval and sign-off of these risk priorities.
- Review existing risk management control strategies noting where the assessed risk level is out of step with the current risk management strategies for that threat.
- Consider appropriate measures to:
 - Transfer the risk e.g. through insurance
 - Accept the risk e.g. where impact / probability are low
 - Reduce the risk e.g. through the introduction of further controls
 - Avoid the risk e.g. by removing the cause or source of the threat
- Ensure that planned risk measures do not increase other risks. For example, outsourcing an activity may decrease some types of risk but increase others.
- Obtain the organisation sponsor's approval, a budget and sign-off for the proposed risk management control (s).

6. Methods and Techniques

The methods, tools and techniques to provide a Risk Assessment include:

Determining threats

- Event Tree Analysis
- Fault Tree Analysis

Assessing probabilities

- Insurance statistics
- Published disaster frequency statistics

Scoring systems

There are many scoring systems in published literature.

Tabulating Threats

- Threat Vulnerability Matrix
- Risk Quartile Matrix

Evaluating solutions

- Cost Benefit Analysis.

7. Outcomes and Deliverables

The outcomes from a Risk Assessment include the identification and documentation of:

- Single points of failure
- Prioritised list of threats to the organisation or to the specific business processes analysed
- Information for a risk control management strategy and action plan for risks to be addressed
- Documented acceptance of identified risks that are not to be addressed

8. Review

A Risk Assessment should be carried out as defined in the organisation's risk management strategy. This may be annually for the most time sensitive processes but more frequently if:

- The pace of business change is particularly aggressive.
- There is a significant change in the internal business processes, location or technology
- There is a significant change in the external business environment - such as market or regulatory change.

Note: BS 25999-1 Section 6.6 (Determining choices) is addressed in Stage 1 – Scope of the BCM Programme

END OF SECTION 2 - UNDERSTANDING THE ORGANISATION



**BUSINESS CONTINUITY
INSTITUTE**

**GOOD PRACTICE GUIDELINES
2008**

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

**SECTION 3
DETERMINING BCM STRATEGY**

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. 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 and 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

At the end of each section there is a summary of "Key BCM Indicators" that will support future use of the BCI Benchmarking Tool, BCI E-Learning and BCI Entrance Examinations.

The view presented in these Guidelines attempts to provide 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. Before referencing this Section of the Guide, you are advised to read Section 1, which explains in more detail how the guide works and how to use it most effectively.

3. About Section 3 - Determining Business Continuity Strategy

Business Continuity Management 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.

Determining Business Continuity Strategy is a key element of good Business Continuity Management. It seeks to build on the detailed analysis in the Understanding The Organisation stage in order to choose appropriate continuity strategies that meet the objectives defined in the BIA. It must support the organisation's objectives, obligations and statutory duties in a cost effective manner.

GUIDELINES STAGE 3:

DETERMINING BUSINESS CONTINUITY STRATEGY

COMPONENTS

3.0 DETERMINING BUSINESS CONTINUITY STRATEGY	4
3.1 DETERMINING BUSINESS CONTINUITY STRATEGY	5
3.2 ACTIVITY CONTINUITY OPTIONS	8
3.3 RESOURCE LEVEL CONSOLIDATION	18

3.0 DETERMINING BUSINESS CONTINUITY STRATEGY

Reference: BS 25999-1 Section 7 & BS 25999-2 Section 4.2

1. Introduction

The first section 'Determining BC Strategy' looks at the general issues of ensuring the protection of the ability of the organisation to deliver a product or service within its Business Continuity programme. The following section describes the tactics available for ensuring the continuity of the activities that support the delivery of products and services.

It also makes sense, where possible, to implement measures to reduce the likelihood of incidents occurring or to mitigate the impact should they fail. However no guidance can be offered here on their cost-effectiveness and they should not be seen as a substitute for the implementation of appropriate BC strategies described below.

In the previous stage the Maximum Tolerable Period of Disruption was discovered for each Product and Services within the scope and, by understanding their interdependencies this will have enabled the MTPD of each activity to be determined. Within the Strategy stage the Recovery Time Objective (RTO) for each activity needs to be set within that MTPD.

3.1 DETERMINING BUSINESS CONTINUITY STRATEGY

Reference: BS 25999-1 Section 7.2

1. Introduction

This section looks at the various high level strategies available to protect product and service delivery.

2. Precursors

A current BIA is a requirement before an appropriate strategy can be selected

3. Purpose

The purpose of this step is to ensure that the overall continuity strategy appropriately supports the delivery of the organisation's product and services.

4. Concepts and Assumptions

Recovery Time Objective

When recovering an interrupted activity the organisation probably will not want to reach the point in time at which it will just survive - it may want to set a (shorter) Recovery Time Objective (RTO) that also gives it a margin in case of unforeseen difficulties with recovery or if its original measurement of MTPD was optimistic.

Continuation or restart capabilities need to be realistic. Physically moving staff and operations will take more time than expected and impact on the available working day. It is important to allow sufficient continuation/restart time into the expected to ensure that business activities can be resumed within the Recovery Time Objectives (RTO).

It is usually the case that the faster the recovery requirement, the greater the cost of a solution. Therefore, to minimise costs, it is important to ensure that an appropriate, but not excessively rapid, RTO is set.

Separation distance - what is off-site?

Since the incidents against which we are planning frequently result in loss of access to or destruction of a location it is necessary to ensure that electronic and other records are duplicated at another geographically separated location in a form that allows them to be accessible and recovered for use within business-defined timescales.

Whilst it is self-evident that greater geographical separation decreases the likelihood of two sites being affected by the same incident, there is no 'minimum' or 'correct' distance for separation as the ability of worldwide infections and computer viruses to cause concurrent incidents demonstrates. However a few hundred metres is likely to provide little protection even in localised incidents because of the way that emergency services use cordons and the likely disruption to transport. Some organisations can use their market or jurisdiction area to define the limit of their dispersion (see discussion of survivable incidents in the Introduction to Stage One); others may choose the pragmatic alternative of placing a relocation site within the limit of how far they judge their staff would travel (which may be about 1 hour away).

Resilience

This term is used to indicate that something can suffer a failure and yet still continue operations. However it is often used as if it were an absolute (e.g. This computer is resilient). However, like the words 'near' or 'far', the term resilience is a relative one whose scope needs to be qualified at each use. This is best illustrated by examples:

- the addition of RAID technology to a computer increases **machine-resilience** (but only to hard-disc failures) and does nothing to protect against loss of that machine in a fire

- duplication of power feeds to a site increases **site-resilience** to power interruptions but the site can still become unusable if the power failure affects both supplies
- Expanding the geographical dispersion and diversity of the organisation's locations increases **organisational-resilience** though it may still succumb to widespread incidents such as pandemics or computer viruses.

5. Process

- Using the results from the Business Impact Analysis, note the Maximum Tolerable Period of Disruption (MTPD).
- Decide on a Recovery Time Objective (RTO) for the product or service, which should (of course) be shorter than the MTPD. This may take into account the confidence one has in the accuracy of the MTPD.
- If there is an existing resumption strategy conduct a 'Gap Analysis' to identify where existing performance is measured against the required performance.
- Provide executive management with a strategic evaluation.
- Ensure the agreed option is 'signed-off' by the executive management including the financial and resource provisions.

6. Methods and Techniques

Issues with specific business services:

Call Centre (s):

A convergence of IT, voice recording and intelligent telephony in a call centre may provide significant recovery challenges. Call Centres handling incoming calls will usually have MTPD measured in hours rather than days so two or more centres geographically dispersed which load share the calls are the usual solution. Due to the typical staff make-up of this type of facility during a sustained period of outage this can present manpower challenges in the event that staff are unwilling or unable to relocate. Some service companies can provide call answering with varying abilities to handle call volumes at varying level of product competence.

Electronic Commerce and Internet / Intranet strategies

These will have a choice based on how the whole organisation views the importance of these services and the role they play - whether for communication only or for interactive business.

The resumption parameters of Electronic Commerce Services need to be determined by a Business Impact Analysis in the same way as other functions. Electronic Commerce Services are often seen as needing rapid resumption because of their visibility and customer expectations.

The Internet and Corporate Intranet may also provide an excellent vehicle for communications during an incident.

Manufacturing solutions

Geographical diversity - manufacturing at more than one site increases resilience to a variety of events but is usually at the expense of economies of scale

Subcontracting - Though each company's total process may be unique, there are usually various processes which can be duplicated by other manufacturers. The affected company can then use a number of subcontractors to produce the usual finished product whilst their own facilities are unavailable. This can rarely be achieved quickly without advance preparation due to the need for tooling and set-up. Unfortunately this strategy may introduce your customers to your competitors.

Warehousing stock - For products that can be stored, an off-site stock can provide a time window in which supply can be maintained while a disruption is resolved.

7. Outcomes and Deliverables

This step will provide a strategy for each product and service under the BCM programme that

will allow the appropriate alternatives for each activity to be selected in the next step.

8. Review

A review of the BCM Strategy for each product and service should be carried out at least every 12 months. However, events may prompt re-examination of the BCM Strategy such as:

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

3.2 ACTIVITY CONTINUITY OPTIONS

Reference: BS 25999-1 Section 7.3-8

1. Introduction

This step covers the process of selecting appropriate tactics for each activity supporting the delivery of one or more products and services within the scope of the BCM programme.

The Business Impact Assessment (BIA) will have identified the MTPD of each activity. Within this time the Recovery Time Objective (RTO) for each activity needs to be set.

Appropriate tactics for each activity must be selected to cover the required resources in the areas of:

- People, skills and knowledge
- Premises
- Technology
- Supplies
- Stakeholders

The options described below are not exclusive of each other. A viable and effective recovery strategy for each activity will need to be built up from elements of all options described.

2. Precursors

The RTO of the product or service needs to be determined before the RTO for each activity is set and the appropriate tactics selected.

3. Purpose

The purpose of this step is to ensure that the tactical continuity options for each activity appropriately support the delivery of the organisation's products and services.

Activities whose resumption is most urgent may be further protected by various threat reduction measures that seem appropriate.

4. Concepts and Assumptions

Reliability

There is often a management decision to be made between the cost and reliability of delivery of a third-party service required for recovery. Promises may vary from verbal promises through 'best endeavours' to a contractually committed service level. Costs may vary (usually correlated to the quality of the promise) from nothing to a substantial sum. The shorter the RTO, the more important the reliability of the delivery becomes.

Extent of planning

The extent and detail to which the tactics for each activity need to be planned will depend on the urgency with which they are required and the complexity of the requirement.

Costs vs. benefits

It is impossible to judge the appropriate cost of measures through conventional cost-benefit analysis since this requires questionable assumptions to be made on the likelihood of incidents to demonstrate the benefit side of the equation.

Manufacturing and service industries who supply other businesses may be able to demonstrate increased sales or better margins can be achieved by demonstrating BCM capabilities (i.e. improved reliability) to their customers - and thus show a benefit to be compared to costs. This is more difficult to demonstrate when the service is non-commercial or is being provided to the public where cost savings on internal processes (reduced disruption) are more likely to be

demonstrable.

Syndication Ratios of third party recovery sites

A "Dedicated" work area is where a subscriber has exclusive use of accommodation. This is generally used where a rapid RTO is required, for high value-generating functions, where specialist equipment is used or where the non-availability associated with syndicated space is judged unacceptable. An example would be dealing desks for an investment company.

A "Syndicated or Subscription" work area is where a subscriber pays for the use of accommodation provided that it is not already in use by a prior invocation by another subscriber.

For syndication the general industry ratio is a maximum of between 40 & 25 to 1 i.e. each desk is sold a maximum of up to 40 times, but great care should be taken to understand who are the other customers potentially using each desk e.g. some suppliers provide client details by post code. The parameters acceptable to an organisation should be clearly defined within its BCM resource recovery strategy and should not be left to individual contract negotiations.

At the current time there are two bases on which a recovery supplier may allocate the available resources to subscribers during a concurrent invocation:

- First come, first served: The first subscriber to invoke the service gets their full allocation of resource; any remainder is available to subsequent subscribers
- Equitable share: The available resources are allocated in proportion to the resources subscribed to.

5. Process

The process includes the following steps:

- Identify possible tactics for each activity that can meet the RTO.
- Select the most appropriate based on cost, guarantees, additional benefits and other factors
- Create and an implementation project for the measure selected.
- Implement an on-going process to ensure the Activity level BCM tactics are reviewed.

Select appropriate tactics from those below.

People, workforce, skills and knowledge

Reference: BS 25999-1 Section 7.3

Techniques for the protection of the organisation's knowledge and skills can provide some protection against loss or absence of key staff:

- Process mapping and documentation - to allow staff to undertake roles with which they are unfamiliar
- Multi-skill training of each individual
- Cross-training of skills across a number of individuals
- Succession planning

Additional skills may be available by permanent or occasional use of third party support. Reliance on this support should be backed by contractual agreements.

The organisation should be protected by a knowledge management programme, which should utilise off-site storage for protection of data.

An organisation could conduct an inventory of staff skills not utilised within their existing roles. These may include:

- First-aid training
- Experience in other roles from other employment
- Salvage
- Leadership or management of a previous incident

Geographical separation of individuals or groups with core skills can reduce the likelihood of

losing all those capable of undertaking a specific role.

Premises

Reference: BS 25999-1 Section 7.4

The RTO is the principal determinant of the appropriate work site continuity tactics.

- An RTO of several months may allow the organisation to choose to leave any decisions until after the event.
- An RTO of over a day or two may allow time for staff to be relocated to another site
- An RTO of less than a day will require tactics that enable the activity to be taken on by staff at other locations - which implies the immediate availability of the resources required by that activity at the other site including current information

Once the RTO parameter has been satisfied, cost and availability will guide the choice of tactics.

The organisation's geographical spread may influence the choice of alternative facilities. Though other company locations may be preferred, staff may be unwilling to travel that distance.

A site with a large number of staff may require more than one alternative location to provide the required capacity. The organisation's future location strategy could be influenced by the availability of suitable nearby in-house alternatives or of third-party sites.

Organisations that provide services to a particular locality, such as public bodies or businesses serving a local market, may be constrained in their choice of alternative locations by the need to be close to their customers.

Facility tactics include:

Do nothing :

- A 'do nothing' strategy may be acceptable for the least urgent activities identified in the BIA. Where the organisation has identified that an activity has a RTO greater than a few months this gives time for buildings to be found and utilities to be installed post-incident with minimal planning and preparation. This option might be made more rapid or reliable by maintaining a current register of suitable buildings available.

Tactics involving relocation of staff to other sites

- *Budge up* makes use of existing in-company accommodation such as a training facility or canteen to provide recovery space or increasing the office density. This will require careful planning and some technical preparation.
- *Displacement* involves the displacing staff performing less urgent business processes with staff performing a higher priority activity. Care must be taken when using this option that backlogs of the less urgent work suspended do not become unmanageable.
- *Remote Working* includes the concept of "working from home" and working from other non-corporate locations e.g. hotels. Working from home can be a very effective solution but care must be taken to ensure Health and Safety issues are addressed and sufficient dial-up capacity is available.
- *Reciprocal agreements* can work in some selected services but care must be taken when establishing this type of agreement. Procedures must be in place to ensure that periodic checks are performed to ensure that the required arrangements have not changed. Reciprocal agreements must have a clause in the contract to ensure that testing is allowed.
- *Third party alternative site* arrangements from a commercial or service company may be an option for consideration if these can ensure the organisation's recovery time objectives (RTO) are achieved. There are a range of commercial services including fixed, mobile and prefabricated sites.
 - o Dedicated space provides guaranteed and immediate availability but is more expensive

- o than syndicated space.
- o Syndicated space usually provides access within 4 hours but may take more than 48 hours for a large number of staff to become productive from the site (Issues with syndication are discussed under Concepts)
- o Mobile facilities can be in use rapidly but provide limited space and may require service connections and significant preparation of foundations
- o Prefabricated units take a minimum of 4 days to build (average 8) assuming pre-prepared foundations and depending on site and weather conditions

Diverse locations - moving the activity (not the staff)

Resilient Operations include dual site operations and continuous availability solutions. In the event of an interruption at one site the business activity is transferred to one or more alternate locations at which staff and facilities are already prepared to handle it.

This last option is normally amongst the more expensive to implement (due to the costs of synchronising data at multiple sites and the overhead of supporting multiple sites) but provide the appropriate solution where quick (less than 24 hour) resumption is necessary. To be a viable recovery strategy this configuration should have no single points of failure and an appropriate geographical separation and diversity of the two or more sites.

Figure: Summary of Relocation Strategies against recovery time

Ownership:	<i>In-house</i>	<i>Contracted</i>	<i>Ad-hoc</i>
Recovery Time:			
<i>Months</i>	<ul style="list-style-type: none"> • Rebuild or relocate 	<ul style="list-style-type: none"> • Extend commercial recovery site contract (if permitted) 	<ul style="list-style-type: none"> • Rebuild, Rent or Purchase
<i>Weeks</i>	<ul style="list-style-type: none"> • Prefabricated buildings on site • Adapt buildings from other uses 	<ul style="list-style-type: none"> • Expansion at Recovery Site • Contracted prefabs and mobile units 	<ul style="list-style-type: none"> • Furnished Offices • Subcontract processes
<i>Days</i>	<ul style="list-style-type: none"> • In-house Recovery Site • Budge-up • Home-working 	<ul style="list-style-type: none"> • Commercial recovery site • Reciprocal Agreements • Mobile facilities • Subcontract processes 	<ul style="list-style-type: none"> • Managed Offices (if available)
<i>Hours</i>	<ul style="list-style-type: none"> • Diverse locations with staff redeployed from other tasks 	<ul style="list-style-type: none"> • Relocate a small team ONLY to contracted commercial recovery site* 	<ul style="list-style-type: none"> • None
<i>Immediate</i>	<ul style="list-style-type: none"> • Diverse locations for each activity 	<ul style="list-style-type: none"> • Initiate contracted 'switch-over' of IT only at commercial recovery site 	<ul style="list-style-type: none"> • None

*Access is available within a few hours but logistics and welfare issues make it unlikely that operations can be resumed reliably within a day or two.

Supporting technologies

Reference: BS 25999-1 Section 7.5

Data Centre(s)

The cost of the solutions and the widespread and rapid impact of the loss of a data centre can have a major financial impact on an organisation.

There are a number of options that can provide a suitable solution including in-house resilience, recovery or third party support.

- Technology duplication at separated locations is required when resumption timescales are short, but this increases in expense according to the degree of duplication.
- Technology recovery provides replacement through third-party contracts

The decision whether to duplicate or contract hardware in advance or acquire it post-incident must take into account the expected lead-time for acquiring the items in a widespread incident. This lead time could be long when less-prepared organisations may be chasing the same equipment. Verbal promises by a supplier to keep a contingency stock should be treated as non-contractual.

There is often a budget conflict between:

- the desire to increase machine-resilience (to minimise downtime due to failure of that machine)
- the need for geographical diversity (which minimises the downtime when the machine, or the building it is in, does fail).

'Ship in' Contracts

This can include generators, IT equipment such as PCs, servers and printers and specialist hardware and equipment such as telephony systems. This may be an appropriate strategy if an unprepared building is to be equipped to provide an appropriate working environment. Most ship-in contracts permit the delivery location to be nominated at invocation, allowing a more flexible response to a specific incident compared to a fixed site recovery capability. Contract terms vary from 'best efforts' to guaranteed delivery.

Telephony

The unplanned redirection of telephony to alternative locations may not be possible within an acceptable timescale particularly during wide-area events. Most telecommunications operators will offer, for a charge, a range of flexible planned solutions that will allow instantaneous or rapid redirection of calls from one site to one or more alternatives. The logistical problem of handling telephone calls during an interruption, once they have been redirected, needs to be addressed.

Techniques include:

- Broadcast notification to staff and other stakeholders
- Non-geographic numbers
- Call diversion
- Resumption plan
- Managed network services
- Mobile switchboard
- Site resilience
- Network resilience

The convergence of telephony and data networks VoIP (Voice over IP) creates new opportunities and continuity issues since telephones and e-mail are often used as alternatives if one fails, These issues need to be assessed and the risks and impacts thoroughly analysed.

Manufacturing equipment

Few options exist for third-party provision of 'ship-in' manufacturing equipment following its breakdown or loss yet there are often long lead-times on its replacement.

Possible techniques to consider are:

- Asset restoration firms may be able to restore the equipment after damage by fire or water
- On-site maintenance or maintenance contracts with firms in the vicinity (to minimise travel delays)
- Use of local subcontractors or competitors with similar equipment Information

Information

Reference: BS 25999-1 Section 7.6

Just because an incident occurs it does not mean that regulatory, statutory or business standards for information management are suspended. Key issues to address are:

Confidentiality

Measures should be taken to ensure that the required level of confidentiality of data is maintained in circumstances such as:

- damage at a location - for example, an explosion may result in the scattering of documents into the street
- successful hacking, which could expose information over the Internet
- use of temporary staff
- sharing temporary accommodation with other organisations

Integrity

Unless back-ups are taken at the same time across multiple connected systems, when restored the data may lack integrity across the various datasets. For example a new order may be present on the order database but the corresponding new customer may not be on the customer database if that was backed up earlier. Time should be allowed within the Recovery Time Objective to allow data issues to be resolved in case they hamper user recovery.

Partial destruction of paper records may hamper recovery where it is uncertain what is missing

Availability

Information required to rebuild equipment or recover and run business processes will need to be available at the time needed to achieve the resumption timescale

There may be statutory requirements for access to documents or data within a specific timescale following enquiries by the public or authorities

Currency

The appropriate back-up strategy for a data set is determined by:

- The amount of data that the users can cope with without fatally hampering their ability to resume their processes
- The impact of the loss of data where the users are outside the organisation - such as customers or regulators
- The speed at which the data can be made available for use after resumption. Data back-up regimes are often designed to minimise back up time; during recovery the speed of restoration is more important. For example logging incremental (daily) changes minimises back up time; differential (changes since last full back-up) takes longer to back-up but is quicker to restore.

There are many methods of data replication across computer systems. These include:

- Mirroring - theoretically zero data loss
- Shadowing - minimal data loss
- Logging - data loss measured in minutes

Each has characteristics of potential data loss, costs, operational distance and reliability that should be compared with user requirements.

Remote storage of duplicate records (paper and electronic)

Paper records storage solutions include off-site managed document stores and optical (scanned) copies.

Electronic record storage can be managed in-house but is also provided by a range of suppliers (often called data vaulting). Records can be sent off-site by physical collection of storage media or by electronic transmission.

The storage site should be sufficiently far away to ensure that the facility is not also affected by an incident, but not so far that access takes so long that RTO's are threatened. Some papers may be work-in progress and be required in short timescales whilst other may be archives retained for legal or regulatory purposes for which deep storage, at lower cost, will be suitable.

- 'Fire-proof' cabinets may be used but do not provide acceptable protection for single copies - even if the contents survive the incident, the safe may not be accessible.
- The original of some documents may be the only one legally acceptable.

Equipment and supplies

Reference: BS 25999-1 Section 7.7

The organisation needs to determine what equipment and supplies are required and how quickly they need to be available following a disruption to meet the RTO of the activity.

Techniques for equipment replacement include:

- Storing additional supplies at another location -
 - if the supplies degrade over time (e.g. paper) then they should be rotated with regular stock
 - changes in the process may require the stored supplies to be changed (e.g. headed stationery if the address or contact details change)
- Arrangements with third parties for delivery of stock at short notice

- Diversion of just-in-time deliveries to other locations
- Holding of materials at warehouses or shipping sites
- Transfer of sub-assembly operations to an alternate location either in-house or to a sub-contractor
- Holding of older equipment as emergency replacement or for spares - at an off-site location
- Specific risk mitigation strategies for unique or long lead-time equipment - where possible outdated equipment should be replaced otherwise its updated replacement may threaten recovery times
- Geographical diversity of processes where the RTO cannot be met by replacement if all equipment is lost in an incident

Techniques for reducing the impact of supply interruptions include:

- Dual or multi-sourcing of materials
- Inspection of supplier's business continuity plans and test performance record and may include a requirement for certification against BS 25999
- Holding inventories off-site - at another site or at the supplier's site
- Significant penalty clauses on supply contracts (though this will not protect against bankruptcy)
- Identification and pre-acceptance of alternative suppliers

Stakeholders, partners and contractors

Reference: BS 25999-1 Section 7.8

There may be many individuals and groups affected by an incident. For example in a major fire at your site there may be contractors injured, local residents evacuated from their homes and local business having to close for safety reasons or suffering reduced trade. The organisation's level of responsibility (both legal and moral) for these groups should be understood.

The organisation should ensure these various stakeholder's needs are satisfied or they may impede the subsequent recovery effort. For example, the local residents could press the local authorities to refuse you permission to rebuild on the site following a fire.

Civil emergencies

Reference: BS 25999-1 Section 7.9

The organisation should be familiar with the procedures of the local emergency responders.

Contact with these groups in advance may provide useful information to assist in an incident such as:

- Recommendations for suitable assembly points and evacuation routes
- Notice of specific hazards in the vicinity
- Likely position of any traffic cordons (in major settlements these may be predefined because of the pattern of the road network)
- Special access arrangements
- Participation in exercises

Civil emergency responding organisations should conduct their own Business Continuity programme to ensure that disruption to their facilities does not hamper the response service they provide to the community. In the UK this planning is a statutory requirement and local government is required to provide BC guidance to commercial and voluntary organisations within their jurisdiction.

Specific threat reduction measures

The BC Manager should be familiar with a number of threat reduction techniques that can provide protection of business activities against certain types of disruptions. Risk assessment may be used to justify which measures are adopted. They include:

- *Physical security* - Advice can be sought from the various national and international

- professional security associations, many who publish guidelines and best practice.
- *Information security* - Advice can be sought from the various national and international ICT and Information Security bodies. ISO 17799 and ISO 27001 would also provide valuable guidelines to follow.
 - *Monitoring systems* may provide prompt warning of utility failures, equipment failures and destructive threats
 - *Uninterruptible Power Supply (UPS)* and back-up generators can protect buildings or specific equipment from power failures. They need to be maintained and tested regularly to ensure performance when required. There are also specialist recovery contracts that will supply portable generators either as a contracted service or on demand (subject to availability).
 - *Sprinkler and Fire Suppression systems* are often advised for buildings with high loading of flammable materials or expensive equipment. Whilst water can put out fires effectively, it can cause considerable damage to papers and electronic equipment whether released correctly during a fire or incorrectly when triggered maliciously or by an explosion or earthquake.

Impact mitigation measures

Insurance, when properly arranged, can provide financial compensation for loss of assets, increased costs of working and protection for associated legal liabilities. However it may not provide cover for the full expense of an incident or damage including the loss of customers, impact of shareholder value or loss of reputation and brand image. The BC Manager should work closely with the Insurance Manager to dovetail insurance cover with BCM parameters,

- An 'All Risks' type Policy will compensate for the assessed value of the damaged or lost physical assets and electronic records.
- Business Interruption insurance may pay for either the "increased cost of working" during resumption or for 'loss of profits' over the disrupted period.
- 'Keyman' insurance may provide a sum following the loss of named individuals from the business due to death, injury or resignation.
- Liability insurance may provide protection for liabilities incurred including those *associated with employees and third-party property and people*.

Asset restoration services are provided by a range of specialist companies who can often minimise damage after fire and flood to papers, equipment and buildings. These firms may provide an advance registration service and advice, as well as being available on request post incident.

6. Methods and Techniques

The tools available to select appropriate tactics include:

- Results from the Business Impact Analysis and Risk Assessment
- Cost Benefit Analysis
- Service and process mapping

7. Outcomes and Deliverables

The outcomes and deliverables from the Activity Continuity Options step include:

- A documented selection of continuity options for each activity, agreed and 'signed-off' by the organisation's executive management.
- A project plan for implementing the agreed strategy.

8. Review

A review to ensure that the appropriate continuity options have been selected for each activity 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 identifies changes in business processes or priorities.

A significant change in the following:

- key technology, telecommunications, accommodation, staffing, service suppliers
- acquisition or merger, new products or services
- regulatory or legislative requirements

3.3 RESOURCE LEVEL CONSOLIDATION

1. Introduction

Having selected appropriate tactics for resumption of each business activity the BCM team will be required to consolidate the resource requirements, determine how to source them and implement their inclusion in the Business Continuity Plans.

2. Precursors

The parameters for resources for each activity will be derived from the Recovery Time Objectives and the numbers or scale determined from the Continuity Requirements Analysis.

3. Purpose

The purpose of this step is to co-ordinate and provide a predetermined level of resources within a Business Continuity Plan (BCP) to enable the implementation of the continuity options selected for each activity.

This consolidation is necessary for two practical purposes:

- If resources are to be purchased then a better price is likely to be achieved with a single order rather than several smaller invitations to tender
- Co-ordinating the acquisition of resources can prevent conflicts - such as when more than one activity within a building expects to use the same alternate workspace at another site.

4. Concepts and Assumptions

Availability of solutions

It is possible that the contracted recovery services required by the business processes do not exist in the vicinity. Some organisations have decided to provide their own recovery facilities, then offer to share them (commercially) with other companies faced by the same dilemma.

5. Process

This process includes the following stages:

- Aggregate Resource Recovery requirements from the Continuity Options section
- Evaluate the costs and benefits for each option for delivering the required solution that can satisfy the recovery time objectives and scale
- Provide executive management with a strategic evaluation of the options
- Ensure the agreed options are 'signed-off' by the executive management including the financial and resource provisions.
- Create an implementation project and action plans
- Apply the agreed strategy to implement the project and action plans (including the development of BCP).
- Implement an on-going process to ensure the resource level BCM planning is reviewed.

6. Methods and Techniques

The tools used to select appropriate solutions from those listed above to create a Resource Recovery Strategy include:

- Results from the Business Impact Analysis and Resource Recovery Analysis as refined by the Process Level Recovery Strategy
- Evaluation tools for purchasing services including value-for-money and contractual terms assessment
- Cost Benefit Analysis

7. Outcomes and Deliverables

The outcomes and deliverables from a Resource Recovery Business Continuity Management Strategy include:

- A set of recovery resources and services which can be deployed under the control of the BCP that provides for the restoration of acceptable functionality for business activities:
 - Within their Recovery Time Objective (RTO)
 - With information recovered to within their Recovery Point Objectives (RPO).

8. Review

A review of the Resource Recovery BCM Strategy should be carried out every 12 months. However, events may prompt re-examination of the BCM Strategy such as:

- Changes in an activity's recovery requirements
- A significant change in accommodation, staffing or available technology that may provide alternative resumption strategies
- A change in the availability of recovery services in the vicinity such as closure, merger or opening of a facility

END OF SECTION 3 - DETERMINING BCM STRATEGY



**BUSINESS CONTINUITY
INSTITUTE**

**GOOD PRACTICE GUIDELINES
2008**

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

**SECTION 4
DEVELOPING AND IMPLEMENTING
A BCM RESPONSE**

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. 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 and 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**

At the end of each section there is a summary of "Key BCM Indicators" that will support future use of the BCI Benchmarking Tool, BCI E-Learning and BCI Entrance Examinations.

The view presented in these Guidelines attempts to provide 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.

Before referencing this Section of the Guide, you are advised to read Section 1, which explains in more detail how the guide works and how to use it most effectively.

3. About Section 4 - Developing & Implementing a BCM Response

Business Continuity Management 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.

Determining and Implementing a BCM response is key to success or failure of a BCM programme. It covers the development of appropriate detailed action plans to ensure continuity of activities and effective incident management.

GUIDELINES STAGE 4:
DEVELOPING AND IMPLEMENTING A BCM RESPONSE

COMPONENTS

4.0 DEVELOPING & IMPLEMENTING A BCM RESPONSE	4
4.1 INCIDENT RESPONSE STRUCTURE	5
4.2 INCIDENT MANAGEMENT PLAN	7
4.3 BUSINESS CONTINUITY PLAN	13
4.4 ACTIVITY RESPONSE PLANS	16

4.0 DEVELOPING & IMPLEMENTING A BCM RESPONSE

Reference: BS 25999-1 Section 8 & BS 25999-2 Section 4.3

1. General Principles

The aim of the various plan (s) covered in this stage is to identify, as far as possible, the actions that are necessary and the resources which are needed to enable the organisation to manage an interruption whatever its cause.

The key requirements for an effective response are:

- A clear procedure for escalation and control of an incident (incident response structure)
- Communication with stakeholders
- Plans to resume interrupted activities

These outcomes can be achieved by various means and only one possible structure is described here. Whatever structure is adopted it is important that the chosen strategy fits with the culture of the organisation.

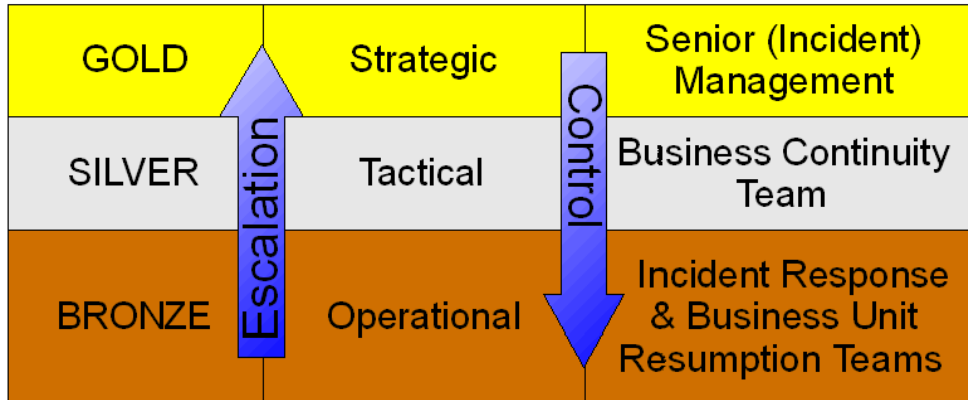
The actions outlined in plans are not intended to cover every eventually as, by their nature, all incidents are different. Any predefined procedures may need to be adapted with flexibility and initiative by those responsible for implementing the plan to the specific event that has occurred and the opportunities it may have opened up.

4.1 INCIDENT RESPONSE STRUCTURE

Reference: BS 25999-2 Section 4.3.1

1. Introduction

One model of incident response, borrowed from the UK Emergency Services, shows three tiers of incident response often referred to as Gold, Silver and Bronze. When applied to an organisation's response structure the responsibilities are as follows.



Strategic Level - Incident Management Plan (IMP)

The IMP defines how the strategic issues of a crisis affecting the organisation would be addressed and managed by the Executive. This may be when the incident is not entirely within the scope of the Business Continuity Plan. This may include crises that do not result from interruptions, such as a hostile take-over or media exposure and those where the impact is over a wider area than that allowed for in the BCM Strategy - such as a national emergency. The media response to any incident is usually managed through an IMP though some organisations would manage the media under a BCP.

The Incident Management Plan is sometimes called a 'Crisis Management Plan'; however reporting in the media that you have invoked your 'Crisis Management Team' may lead people to think you feel you have a Crisis. The term 'Incident' has less negative connotations so is preferred in this document.

Tactical Level: Business Continuity Plan (BCP)

The BCPs address business disruption, interruption or loss from the initial response to the point at which normal business operations are resumed. They are based upon the agreed Business Continuity Strategies and provide procedures and processes for both the business continuity and resource recovery teams. In particular the plans allocate roles and their accountability, responsibility and authority. The plans must also detail the interfaces and the principles for dealing with a number of external players in the response such as recovery services suppliers and emergency services.

If the event falls outside the scope of the assumptions on which the Business Continuity Plan was based then the situation should be escalated to those responsible for implementing the Incident Management Plan (IMP).

Operational Level: Activity Resumption Plans

For operational departments the plans provide for resumption of its normal business functions. For departments, such as Facilities and IT that are managing infrastructure, the plans will provide a structure for restoring existing services or providing alternative facilities.

Timeline

In an incident the three types of plan will address different issues during the various phases of the event. For example:

<i>Event Phase</i>	<i>Situation</i>	<i>Incident Management Plan</i>	<i>Business Continuity Plan</i>	<i>Business Unit Resumption Plan</i>
<i>One</i>	<i>Immediate aftermath</i>	Media management Strategic assessment	Emergency Services Liaison Damage assessment Formal invocation of BC services	Damage limitation and salvage (Facilities) Casualty management (HR)
<i>Two</i>	<i>Damage contained</i>	Media management Monitoring BC team	Mobilising alternative resources	Staff communication
<i>Three</i>	<i>Resumption beginning</i>	Stood down	Managing alternative resources	Resumption of business critical functions
<i>Four</i>	<i>Consolidation</i>	Review	Stood down Review	Resumption of further functions and projects

Scalability

Whilst the three levels provide a suitable model for a medium sized organisation with a single site a smaller organisation may have a single 'hands-on' management group with both tactical and strategic responsibilities. However it is still important that this single group addresses the strategic issues despite the pressing issues of a tactical response.

For multiple site organisations a variety of models may be appropriate, perhaps with additional tiers beyond the three named above, for example:

- A response team at each site backed-up with a central Business Continuity team
- A Business Continuity team at each major site with a central Incident Management Team
- BCM at a national level with limited involvement from the International Board unless global reputation is threatened

4.2 INCIDENT MANAGEMENT PLAN

Reference: BS 25999-1 Section 8.3-5 & BS 25999-2 Section 4.3.3

1. Introduction

Case studies of major incidents (Knight and Pretty - Oxford Metrica "The Impact of Catastrophes on Shareholders Value" by Rory F. Knight and Deborah J. Pretty. Templeton College of Oxford University, 1996) suggest that effective and rapid management of a crisis is the significant factor in protecting an organisation's brand from financial and reputation damage.

2. Precursors

For organisations with no plans in place, the Incident Management Plan (IMP) may be the first element to develop, providing a limited amount of protection while other plans are developed.

3. Purpose

The purpose of an IMP is to provide a documented framework to enable an organisation to manage any crisis event regardless of cause (including those where no Business Continuity response is appropriate such as a threat to reputation).

4. Concepts and Assumptions

The terms used in these guidelines for the various plans are not universally applied, in particular the term Incident Management Team may be applied to what others would call a Crisis Management or Response team. It is important that an organisation chooses names that fit into its culture and structure, but that the roles described here are covered.

Some incidents will require an IMT response that do not result from disruption to activities for example those involving threats to reputation alone - and may therefore not involve a Business Continuity response. However, where a BC response is required there is almost always a need to involve the IMT if only to make them aware of the situation in case it escalates.

5. Process

The key steps in developing an IMP include:

- Appoint an owner for the Incident Management Plan on the Executive
- Define the objectives and scope of the plan
- Develop and approve a Incident Management plan development process and programme

Note: If no plan exists it may be useful to run an exercise with the senior management team but exerting minimal pressure, so that the many requirements of a plan become apparent such as the need for a plan

- Create an Incident management planning team to develop the plan
- Agree the responsibilities of the Incident Management Team and their relationship with other plans
- Decide the structure, format, components and content of the plan
- Determine the strategies, such as alternative locations, on which the plan is based
- Gather information to populate the plan
- Nominate individuals and deputies (if the senior management team is too large)
- Nominate administrative support for the IMT
- Draft the plan
- Circulate the draft of the plan for consultation and review

- Gather feedback from the consultation
- Amend plan as appropriate
- Agree and validate the plan, for example by using it in an exercise
- Repeat the process for the Incident Communications Plan (if separate)
- Agree a programme of ongoing exercising and maintenance of the plan to ensure it remains current

6. Methods and Techniques

Building the Incident Management Plan

The methods, tools and techniques to enable the planning and development of an Incident Management Plan include:

- Stakeholder analysis
- Scenario planning
- Checklist(s)
- Workshops

IMP Templates for distribution to assist implementation of standard procedures in an international organisation with several IM teams

A variety of software products are available to assist in building and maintaining a Incident Management Plan. They can provide significant benefits in the areas of plan maintenance and referential integrity but they are not necessary and do not replace knowledge of the business.

IMP Contents

As, by their nature, all crises are different, the Incident Management Plan is a set of components and resources that may be useful to the team tasked with activating the plan. The contents will also depend on the nature and complexity of the organisation.

The Incident Management Plan should be modular in design so that single sections can be supplied to individuals and/or teams on a need-to-know basis. It is suggested that the different sections are printed on different coloured paper to provide ease of use at the time of a crisis.

Document owner and maintainer: The plan should have a nominated owner and procedure for maintenance.

Roles and Responsibilities:

The roles of the team and specific individuals should be documented.

Deputies should be identified for each role.

Responsibilities for the team or nominated individuals may include:

- Managing communications (see section below)
- Ensuring IMT and BCT are properly staffed and making appointments if necessary
- Liaising with the Business Continuity Team to agree resumption timetable
- Approving significant expenditure
- Monitoring the overall progress of recovery and personnel performance
- Identifying and maximising opportunities or advantages arising from the incident
- Looking at the strategic impact of the incident on the organisation - which may require significant changes in direction or open up new opportunities
- Maintaining a decision log throughout the incident.

Invocation / mobilisation instructions

The circumstances in which the team will be activated should be documented, and the persons able to initiate the call-out decided. However, due to the nature of incidents, this should allow some flexibility and encourage action where this is doubtful since it is easier to stand down an activated team than activate them after the incident has developed out of control.

The means by which the team will be activated should be documented so that decisions can be made in the shortest possible time.

The team should agree, in advance, a number of possible meeting locations favouring those with the required resources (see below). On invocation the first notified should identify the most suitable meeting place and a fallback, based on the current information.

Action plans

The plan should contain initial prompts for action - such as stakeholder list. The Business Impact Analysis may contain useful pointers to potential impacts that will need to be managed

Meeting room

At least two locations should be predefined to act as an incident management centre (control room or command centre). One is likely to be on-site where the senior management team are based but the other should be designated off-site.

The off-site location does not have to be owned by the organisation. By prior arrangement, a 24-hour hotel should be able to provide all the facilities required for most organisations.

Consideration should be given to how the space is best utilised for the needs of:

- communication - incoming and outgoing
- recording events, actions and issues
- monitoring broadcasting
- controlled entry

Resources

The following resources should be considered:

- Whiteboard/flip charts (and pens that work)
- A number of telephones, including at least one with an ex-directory outgoing line and phone recording facility
- Hotline/helpline facility
- Mobile communicators, cell phones, fax, e-Mail and Internet
- TV and radio monitoring equipment
- TV/radio 'studio' facilities - to rehearse interviews
- Communications line + camera for transmitting interviews straight to broadcast station and videoconferencing
- Stationery
- A means of logging all actions.
- Refreshments and nearby or on-site sleeping facilities
- A separate and nearby venue for hosting the press

Hardware and information can be kept off-site at the alternative location in a locked trunk

(often called a 'battle-box' or 'recovery box').

People Activities

Organisations have a responsibility to safeguard the welfare of their employees, contractors, visitors and customers (which may be legally enforced). All BCM strategies should take into account welfare issues during an incident and the recovery phase. Staff are more likely to cooperate willingly with the extra demands if their welfare needs are met.

Issues to consider in planning include:

- Special needs of individuals during evacuations or stay-in periods including:
 - pregnancy
 - disabilities
 - family responsibilities

During an incident one or more individuals should assume responsibility for:

- Site evacuation
- Accounting for staff, contractors and visitors
- Communicating with staff and others on the site
- Contact with emergency contact or next of kin - local regulations may require that this should only be done in consultation with the emergency services
- Translation services
- Transport assistance
- Setting up a staff help line

Subsequently there may additional needs including:

- Temporary accommodation
- Counselling and rehabilitation services - this could be provided as part of an employee health package
- Welfare needs at alternative locations:
 - Special needs
 - Refreshments
 - Personal safety and security
 - Transport and accessibility
 - Appropriate training on replacement equipment

Emergency services liaison

Staff with an appropriate level of experience and authority should be appointed to liaise with the emergency services at the arrival on site and subsequently as required.

The emergency services should be given information on the location of any casualties and the status of the situation and any known hazards they may encounter.

Whilst on the site, the emergency services instructions take precedence over those given by the organisation's own staff.

On departure from the site, the organisation will resume responsibility for its own site security.

Incident Communications Plan

The Incident Communications Plan should address how the organisation will manage communication with all stakeholders including:

- Staff, relatives, friends and emergency contacts

- Customers and suppliers
- Shareholders or owners
- (If part of a group or larger organisation) liaising with other members of the group or head office
- Informing and liaising with regulatory authorities (following consultation with the organisation's legal and compliance functions)
- Dealing with issues relating to serious injuries or fatalities (in consultation with the Emergency Services and in accordance with local regulations and customs)
- Media - local and national newspapers, radio, TV, internet and other media

Consider in advance:

- What crises could hit us? (A Risk Assessment may be appropriate)
- Who are the audiences?
- How do we communicate with them?
- What are the Messages?
- Who will form the Incident Team?
- What are the Resources and Facilities?
- Are the Incident team and spokespeople trained?
- Does it Work?
- What Incident Manual do we need?
- Have we built lines of communication with our audiences?
- When a crisis or business discontinuity gets into the public domain, effective communication will play a key role in rescuing and maintaining an organisation's most valuable asset - its reputation.

If faced with a crisis consider:

- Ownership of the plan: all those who will have to make decisions about how to communicate must have agreed beforehand on the who, how and what of communication.
- Perception is reality: your reputation is affected not so much by what has happened as by what people think has happened - and by their perceptions of how you handle it.
- Understand your key audiences and what they need to hear.
- Act fast: With every passing hour of silence your reputation problem doubles. You need to seize the communications high ground.
- Be open: give as much information to your various audiences as you legally and practically can. Showing that you have nothing to hide helps to allay suspicion.
- Show you care: see it from your audiences' point of view and tailor your messages to what they need to hear, not just what you want to say.

7. Outcomes and Deliverables

The outcomes of the Incident Management Planning process include:

- An Incident Management Plan that can support the role of the organisation's Incident Management Team during a crisis event
- An Incident Communications Plan that can manage the media and stakeholder communication during a crisis
- Demonstration of preparation for effective Incident management to the media, markets, customers, stakeholders and regulators

- Compliance with statutory, regulatory and ethical requirements

8. Review

The review or audit should be aligned with the review of other BCM and Incident Management related strategies, plans and solutions.

A review of the plan may be triggered by a major business or senior management change or significant change in the external operating environment.

4.3 BUSINESS CONTINUITY PLAN

Reference: BS 25999-1 Section 8.3 & 8.6-7 & BS 25999-2 Section 4.3.3

1. Introduction

The Business Continuity Plan pulls together the response of the whole organisation to a disruptive incident by facilitating the resumption of business activities. Those using the plan should be able to analyse information from the response teams concerning the impact of the incident, select and deploy appropriate strategies from those available in the plan, direct the resumption of business units according to agreed priorities and pass progress information to the Incident Management Team.

The components and content of a Business Continuity Plan will vary from organisation to organisation and will have a different level of detail based on the culture of the organisation and the technical complexity of the solutions.

2. Precursors

It is rarely possible to write an effective Business Continuity Plan unless the key elements of the resumption strategy are in place or are well advanced in their planning.

3. Purpose

The purpose of a Business Continuity Plan(s) is to provide a documented framework and process to enable the organisations to resume all of its business processes within their RTO. A Business Continuity Plan on its own does not demonstrate a BCM competence or capability.

4. Concepts and Assumptions

The plan should be 'action orientated' and should therefore be easy to reference at speed and should not include documentation (for example the BIA) that will not be required during an incident.

The BCP will always contain (and should document) assumptions about the maximum scale of the incident (in terms of extent, duration or staff impact). If these are exceeded then this should be escalated to the Incident Management Team to resolve since the solution will, almost inevitably, involve a strategic decision.

5. Process

The key steps in the development of a Business Continuity Plan are:

- Appoint an owner for the BCP (or each plan for multiple sites)
- Define the objectives and scope of the BCP with reference to the organisational strategy and BCM Policy
- Develop and approve a planning process and timetable programme
- Create a planning team to carry out the plan development
- Decide the structure, format, components and content of the plan
- Determine the strategies which the plan will document and what will be documented in other plans
- Determine the circumstances that are beyond the scope of the BCP
- Gather information to populate the plan
- Draft the plan
- Circulate the draft of the plan for consultation and review
- Gather feedback from consultation process

- Amend the plan as appropriate.
- Schedule ongoing exercising and maintenance of the plan to establish it remains current (see later Section 5)
- Test the plan using a desktop exercise (see later Section 5)

6. Methods and Techniques

A Business Continuity Plan should be modular in design so that separate sections can be supplied to teams on a need-to-know basis. Each section could be printed on different coloured paper to provide ease of use and reference. A further suggestion is to ensure that all regularly changing information - such as contact details are kept in appendices at the back of the plan which can more easily be amended, with job titles rather than names in the text of the document.

A variety of software products are available to assist in building and maintaining a Business Continuity Plan however it is not essential. Using normal office software (Word processor and spreadsheet) may suffice and is more inclusive of all staff since its use does not require special training. Customised software can however provide significant benefits in the areas of plan maintenance and referential integrity.

Whatever the planning solution there must be a clearly defined and documented control and change management process for the production, update and distribution of the Business Continuity Plan.

The plan should contain:

- Document owner and maintainer
- The person or group nominated to ensure the plan remains up to date and effective.
- Roles and Responsibilities
- The roles of the team and specific individuals should be documented. Deputies should be identified for each role.
- Responsibilities of the team or specific individuals may include:
 - Liaising with the Emergency Services
 - Receiving or seeking information from response teams
 - Reporting information to the Incident Management Team
 - Mobilising third-party suppliers of salvage and recovery services
 - Allocating available resources to recovery teams
- Invocation / mobilisation instructions

The circumstances in which the team will be activated should be documented, and the persons able to initiate the call-out decided. However, due to the nature of incidents, this should allow some flexibility and encourage action where this is doubt since it is easier to stand down an activated team than activate them after the incident has developed out of control.

The means by which the team will be activated should be documented so that decisions can be made in the shortest possible time.

The team should agree, in advance, a number of possible meeting locations favouring those with the required resources (see below *Resource Requirements*). On invocation the first notified should identify the most suitable meeting place and a fallback, based on the current information.

Action plans / task list

Detailed procedures for the team to:

- Respond to invocation
- How decisions are to be taken
- Mobilise resources

- Initiate activity recovery
- Receive information from other teams
- Report status to Incident Management team

Resource requirements

Lists of the available resources:

- Personnel
- Facilities and supplies
- Technology, communications and data
- Security
- Transportation and logistics
- Welfare requirements
- Emergency cash and payments
- Contact information to access those resources
- Resource requirements for resumption of each activity

Vital information

- Customer information
- Contact details
- Legal documents - such as contracts and insurance policies
- Service Level Agreements

Forms and annexes

- Checklists to assist recovery

7. Outcomes and Deliverables

The deliverables of the Business Continuity Management planning process include:

- A Business Continuity Plan which should be 'signed-off' by the Executive
- A framework within which Business Unit plans (see Section 5) can operate

8. Review

Some information within Business Continuity Plans such as contact details should be reviewed in line with BC policy. Other information should be formally reviewed annually and tested through exercising. Other triggers leading to a review are:

- A significant change in the technology and/or telecommunications

There is a major business process change

- A significant change in staff
- A change in the supplier of BC solutions

4.4 ACTIVITY RESPONSE PLANS

1. Introduction

A Business Continuity Plan will rapidly become unwieldy if all recovery procedures are included in a single document. When this becomes the case (in medium-sized or large organisations) the response and recovery plans of each activity should be taken out of the BCP and made a separate document that becomes the responsibility of the activity to which it relates.

The Activity (Operational level) Response Plans cover the response by each department or business unit to the incident. Examples of Operational Response plans are:

- Procedures to assist an incident response team usually lead by a Facilities department who deal with the specific incident and its physical impact (if any)
- A Human Resources response to welfare issues in an incident
- A business department plan to resume its functions within a predefined timescale
- An IT department's logistical response to the loss and subsequent resumption of IT services to the business

The complexity and urgency of the business processes may determine whether one operational plans covers a single activity or a department covering several activities.

Depending on the complexity of the organisation, the operational response plans may be supported by more detailed plans for specific responses, locations or equipment.

2. Precursors

Because of the many links between the BCP and those of the operational response, the BCP should be written, at least in outline, before these operational plans are finalised.

3. Purpose

The purpose of the Activity Response Plan is to structure the response of each department to an interruption within the overall Business Continuity Plan.

4. Concepts and Assumptions

The plan should be 'action orientated' and should therefore be easy to reference at speed and should not include documentation that will not be required during an incident.

5. Process

The key steps of the Business Unit Resumption Plan development and planning process include:

- Appoint a person to be responsible for development of the plans overall and a representative within each operational unit to develop their plan
- Define the objective and scope of the plans
- Develop a planning process and timetabled programme. Where possible, begin with the plans for the most urgent business activities
- Determine the overall BCM strategies on which the plan is based.
- Decide the structure, format, components and content of the plans
- Develop an outline or template plan to encourage standardisation of documentation but allow individual variations where this is appropriate
- Ensure that Business Units nominate individuals to fulfil roles within their plans
- Manage and mentor the development of plans within the Business Units
- Circulate the draft of the plan for consultation, review and challenge within and, where

- necessary outside, the department
- Gather feedback from consultation
- Amend plan as appropriate
- Validate the plan through a unit test
- Consolidate the BU plans and review for consistency
- Document connections with the BC Plan and between Unit plans
- Conduct a resource requirements analysis across all plans to define resource requirements for support functions

6. Methods and Techniques

The methods, tools and techniques to develop an Operational Response Plan include:

- Interviews (structured and unstructured)
- A Business Impact Analysis and Resource Requirements analysis for this activity
- Checklists and templates
- Workshops

Specific Response plans may include the following:

- Facilities (Incident Response Team)
- Staff Welfare plans
- Business Unit Resumption
- IT Disaster Recovery

The above plans may include appropriate procedures and information such as:

- Building Evacuation and "Stay-in" plans
- Response to Bomb Threat and similar scenarios
- Evacuation Points (including alternate or off-site)
- Emergency Services Liaison
- Dispersal of staff and visitors
- Salvage Resources and Contracted Assistance
- Escalation circumstances
- Human Resource and Welfare issues
- Health and Safety legal liabilities
- Procedure for accounting for staff
- Procedure for contacting staff
- Counselling and rehabilitation resources
- Escalation criteria
- Escalation procedure to Business Continuity Team (BCT)
- Response to Initial contact from BCT
- Contacting team members
- Resumption Plan for each process
 - Staff numbers
 - Key contacts
 - Procedure for resumption of business activity

- Activity Priorities
- Special procedures
- Work in Progress issues
- Consumables required

7. Outcomes and Deliverables

The outcomes of the Operational Response Plan include:

- A documented Operational Response Plan for each business activity or department
- Criteria for BU to escalate issue to BCT
- Clearly defined BCM roles within the department

8. Review

Operational Response plans should be reviewed if there is a major change in the business process or technology within that area.

END OF SECTION 4 - DEVELOPING AND IMPLEMENTING A BCM RESPONSE



**BUSINESS CONTINUITY
INSTITUTE**

**GOOD PRACTICE GUIDELINES
2008**

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

**SECTION 5
EXERCISING, MAINTAINING &
REVIEWING BCM ARRANGEMENTS**

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. 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 and 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**

At the end of each section there is a summary of "Key BCM Indicators" that will support future use of the BCI Benchmarking Tool, BCI E-Learning and BCI Entrance Examinations.

The view presented in these Guidelines attempts to provide 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.

Before referencing this Section of the Guide, you are advised to read Section 1, which explains in more detail how the guide works and how to use it most effectively.

3. About Section 5 - Exercising, Maintaining & Reviewing BCM arrangements

Business Continuity Management 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.

This section ensures that organisation's BCM strategies, plans and contractual arrangements are validated by exercise and review and that they are kept up to date.

GUIDELINES STAGE 5:
EXERCISING, MAINTAINING & REVIEWING BCM ARRANGEMENTS

COMPONENTS

5.0 EXERCISING, MAINTAINING & REVIEWING BCM ARRANGEMENTS	4
5.1 EXERCISE PROGRAMME	6
5.2 EXERCISING BCM ARRANGEMENTS	8
5.3 MAINTAINING BCM ARRANGEMENTS	12
5.4 REVIEWING BCM ARRANGEMENTS	14

5.0 EXERCISING, MAINTAINING & REVIEWING BCM ARRANGEMENTS

Ref: BS 25999-1 Section 9 & BS 25999-2 Section 4.4

1. General Principles

Exercising

A Business Continuity Management (BCM) capability cannot be considered reliable until it has been exercised. Since it is rarely possible to undertake an exercise for the whole organisation at one time, a planned exercise programme is required to ensure that all aspects of the plans and personnel have been exercised over a period of time.

Exercising can take various forms, including technical tests, desktop walk-throughs and full live exercises. No matter how well designed and thought-out a BCM Strategy or BCP; a series of robust and realistic exercises will identify issues and assumptions that require attention.

Time and resources spent exercising BCM Strategies and BCPs are crucial parts of the overall process as they develop competence, instil confidence and impart knowledge that are essential at times of crisis.

Though effort needs to be put into testing technical recovery capabilities, the key element is the role of people and their resilience in skills, knowledge, management and decision making.

While a service or activity may be outsourced, the risk accountability cannot. Consequently organisations must assure themselves of the readiness of suppliers of outsourced services to cope with disruption, by exercising their own plans and requiring evidence of the viability of their suppliers contingency plans and the testing of them.

Maintenance

Most organisations exist in a dynamic environment and are subject to change in people, processes, market, risk, environment, geography, and business strategy. To ensure that their BCM capability continues to reflect the nature, scale and complexity of the organisation it supports, it must be current, accurate, complete, exercised and understood by all stakeholders and participants.

A Business Continuity Maintenance Programme must be established to ensure that all relevant stakeholders have the current and relevant parts of the BCP.

Review

There are several ways to review a BCM programme including:

- Internal audit
- External audit
- Self-assessment

The BCM Audit process ensures that an organisation has an effective Business Continuity Programme. Audit has five key functions:

- To validate compliance with the organisation's BCM policies and standards
- To review the organisation's BCM solutions.
- To validate the organisation's BCPs.
- To verify that appropriate exercising and maintenance activities are taking place
- To highlight deficiencies and issues and ensure their resolution.

The Audit process can be undertaken by an organisation's Internal Audit function, an External Auditor, or External Professional BC Practitioner. The process should be conducted annually or biannually. In the interim, self-auditing, or 'Performance Monitoring' may be carried out more frequently, by the owners of the BC plans.

5.1 EXERCISE PROGRAMME

Ref: BS 25999-1 Section 9.2

1. Introduction

The development a BCM capability is achieved through a structured exercising programme.

To be successful an exercising programme must begin simply and escalate gradually.

Where the delivery of a product or service has been outsourced the responsibility for delivery remains with the original organisation. In this case the organisation should assure itself, through exercising, that the outsource company is able to deliver its obligations. Similarly suppliers of products or services whose failure would cause significant disruption to the organisation should be asked to demonstrate their recovery capability.

2. Precursors

The BCM Policy should outline the timetable and responsibilities for the exercise programme.

3. Purpose

The purpose of the exercise programme is to ensure that over a period of time:

- All information in plans is verified
- All plans are rehearsed
- All personnel (including deputies) are exercised

4. Concepts and Assumptions

Outsourced activities

The exercising of outsourced activities should be made a requirement of the contract and be enforced through service level agreements.

5. Process

- Draw up a list of all recovery processes (e.g. call-tree, relocation)
- Decide on suitable type of exercise activity for each process
- Draw up a list of all personnel or groups involved in each process
- Devise a timetable of exercise activities that ensures that, over a period, all relevant personnel are included in the exercise activity

Recovery processes

The exercise programme should include suitable activities to exercise the various facets of the BCM strategies adopted. These may include:

- Technical - does the equipment work
- Procedures - are the procedures correct
- Logistical - do the procedures work together in a logical fashion
- Timeliness - can the procedures achieve the required RTO for each activity
- Administrative - are the procedures manageable
- Personnel - are the right people involved and do they have the required skills, authority and experience

6. Methods and Techniques

A progression and potential combinations of exercises are illustrated in the following matrix:

Type of Test			High	Low
Desk Check	Check the contents of the plan as a precursor to maintenance	Author of plan Another manager (verification)	^	^
Walk through	Carry out an extended desk check to check interaction and roles of participants	Author of plan Main participants		
Simulation exercises	Incorporates associated plans: Business plans Buildings Communication	Main Participants: Observers Co-ordinators		
Activity testing	Moves work to another site. Recreates the existing work from the displaced site	Employees in a business area Hot site suppliers Observers Co-ordinators		
Full test	Shuts down an entire building and relocates work	All employees in a building Hot site suppliers Co-ordinators Observers	V	V
			Low	High

Figure : Exercising types (from the AA) (Source: Elliot, Swartz and Herbane 1999 p.84)

7. Outcomes and Deliverables

The outcomes of the BCM exercising programme process include:

- A timetable for an exercise programme

8. Review

The frequency of a BCM Exercise Programme is dependent upon the nature, scale and complexity of the organisation. An exercise of the organisation's overall BCM capability should take place at least once every 12 months. Other events, which may require an exercise to be scheduled, include:

- A significant change in the processes, staff or technology
- There is a major external business environment change

5.2 EXERCISING BCM ARRANGEMENTS

Ref: BS 25999-1 Section 9.3

1. Introduction

Exercising is a generic phrase used here to describe the exercising of Business Continuity Plans, rehearsing team members and staff and testing of technology and procedures. Three terms are in general use:

- Test: Usually used when a technological procedure and/or business process is being tried, often against a target timescale. In this sense the result can be either a 'pass' or 'fail' (for the procedure, not the individual). An example is the rebuilding of a server from back-up tapes.
- Rehearsal: A practice of a specific set of procedures that require the following of a script to impart knowledge and familiarity. An example is a fire drill
- Exercise: Usually for a scenario-based event when decision-making abilities are being examined. An example is a desktop exercise to manage a major incident.

Regardless of the term used, it is important to demonstrate that an exercise is an opportunity to measure the quality of planning, competence of individuals and effectiveness of capability rather than a simple 'pass or fail' examination. A positive attitude towards BCM exercising makes the process more acceptable and enables strengths to be acknowledged and weaknesses to be seen as opportunities for improvement rather than criticism.

2. Precursors

An individual exercise activity should form part of an exercise programme and may need to be scheduled with supporting training activities.

3. Purpose

The purpose of exercising is to:

- Evaluate the organisation's BCM current competence.
- Identify areas for improvement or missing information
- Highlight assumptions which need to be questioned
- Provide information and instill confidence in exercise participants
- Develop team work
- Raise awareness of Business Continuity throughout the organisation by publicising the exercise.
- Test the effectiveness and timeliness of restoration procedures at the end of the exercise.

4. Concepts and Assumptions

In order for any test to be "useful", it needs to meet the following criteria: Stringency, Realism, and Minimal Exposure. These three criteria often have conflicting requirements, and will require a compromise to be reached between them.

Stringency

Tests should be carried out, wherever possible, using the same procedures and methods as would be used in a real event, making the event as real as possible. This is the ideal, but it may not be possible to run certain tests without alterations to "live" procedures. This applies especially to technical testing.

Realism

The usefulness of a test is reduced by the selection of an unrealistic scenario. The simulation of an event is needed to prove the viability of plans in such circumstances.

The setting of a realistic business scenario ensures that the audience engages fully in the event and ultimately gains more from it.

Minimal Exposure

Testing may place the business at a level of increased risk. The designer of the test should ensure that:

- the risk and impact of disruption is minimised
- the business understands and accepts the risk

For more complex technical tests, the test manager should ensure that there are agreed stop/go points at key stages throughout the test, and adequate back-out plans in case of things going wrong.

Similarly for desktop or live exercises the exercise manager requires the capability to call a time out during the event if the team is making decisions that would not be appropriate in the given scenario.

5. Process

A technical test may include the following steps:

- Agree the scope and objectives of the test
- Agree budget for the test if required
- Assign appropriate personnel to the task
- Devise a simple scenario and set of assumptions that puts the test in context
- Conduct a Risk Assessment of the test to minimise the risk of an impact on live operations
- Conduct the test and record the results
- Assess and report the results
- Address any issues raised

A scenario exercise will require similar steps though each will be more complex:

- Agree the scope and objectives of the exercise with senior management
- Agree the budget for the test
- Agree with the appropriate managers of the organisation and any suppliers of logistics/services required to enable the exercise to take place
- Prepare a realistic and suitably detailed scenario
- Include aspects such as date, time, current workload, political and economic conditions and temporal/seasonal issues
- Ensure required participants are available
- Conduct a Risk Assessment of the exercise to minimise the risk of an impact on live operations
- Brief observers and prepare questionnaires for use during the exercise to capture lessons learned by all players and observers
- Pre-exercise information and briefing of participants
- Conduct the exercise
- Debrief participants immediately after the exercise

- Conduct a formal debrief at a later date
- Evaluate exercise and debriefing results and prepare a Post Exercise Report and recommendations.
- Prepare an open-issues report during and immediately following the test
- Circulate reports to participants and senior management
- Circulate report to participants and senior management
- Create an action plan to implement post exercise report recommendations i.e. update the strategy and plan as approved, review exercising schedule for further exercising to prove the efficacy of the changes.

6. Methods and Techniques

Participants

Possible participants, in addition to staff, in desktop or scenario exercises include:

- Facilitator
- Suppliers of specialist BCM resources and services
- Insurance representatives
- Emergency Services
- Security
- Local Authority Emergency Planning Officer
- Communications and Public Relations
- Subject Experts (where appropriate)
- Suppliers of business services/products
- Outsourced activity providers

7. Outcomes and Deliverables

The outcomes of the BCM exercising process include:

- Validation that the Business Continuity strategies are effective
- Familiarity of team members and staff are familiar with their roles, accountability, responsibilities and authority in response to an incident
- Testing of the technical, logistical, administration aspects of the Business Continuity Plan(s)
- Testing of the recovery infrastructure that includes command centres, work area, technology and telecommunications resource recovery
- The rehearsal of the availability and relocation of staff
- Documentation of exercise results in a Post Exercise Report for senior management, auditors, insurers, regulators and others
- Documentation and resolution of open-issues arising during the exercise
- An increased awareness of emergency procedures
- An increased awareness of the significance of BCM
- The opportunity to identify shortcomings and improvements to the organisation's Business Continuity readiness

8. Review

The frequency of a BCM Exercise Programme is dependent upon the nature, scale and complexity of the organisation. An exercise of the organisation's overall BCM capability should take place at least once every 12 months. Other events that may require an exercise to be scheduled include:

- A significant change in the processes, staff or technology
- There is a major external business environment change

5.3 MAINTAINING BCM ARRANGEMENTS

Ref: BS 25999-1 Section 9.4

1. Introduction

The BCM Maintenance Programme ensures that the organisation remains ready to handle incidents despite the constant changes that all organisations experience. To be effective the BCM Maintenance Programme should be embedded within the organisation's normal management processes rather than be a separate structure that can be forgotten.

2. Precursors

Most of the issues that show up in tests and exercises are the result of internal changes within the organisation - staff, locations or technology.

3. Purpose

The purpose of the Business Continuity and Incident Management maintenance process is to ensure that the organisation's BCM capability remains effective despite changes to internal business processes and external influences.

4. Concepts and Assumptions

An effective change management process is a prerequisite of maintenance of the BCM program.

5. Process

Review internal changes to

- Business processes
- Technology
- Staff

This review may be triggered by the change management process highlighting the change, by post exercise 'learning points' action plan or an audit report.

- Review and challenging the assumptions made in the BIA about the environment in which the organisation operates to determine whether the time imperatives have changed since the last review
- Review the adequacy and availability of external services that might be required by an organisation in times of difficulty such as asset restoration, recovery sites and subcontracts
- Review the Business Continuity arrangements of suppliers of time-critical components to the business
- Assess whether changes and amendments create a training, awareness and/ or communication need.
- Deliver appropriate training, awareness and/ or communication where applicable.
- Distribute updated, amended, changed BCM policy, strategies, solutions, processes and plans to key stakeholders under the formal change (version) control process.

6. Methods and Techniques

- Each plan owner is responsible for updating the team's BC plans and dynamic data such as staff out-of-hours contact numbers, team tasks, notification and supplier contact details, contingency-box contents etc.
- Plan sections are updated at frequencies ranging from monthly to annually, in accordance

with the schedule laid down in the BC Plan Maintenance Chapter/Section. The appropriate update months are also specified in the BC Plan Maintenance Chapter/Section.

- 'Date of last update' is clearly displayed at the beginning of each BC plan Chapter/Section to provide an effective audit trail.

7. Outcomes and Deliverables

The outcomes from the BC maintenance process include:

- A documented BC monitoring and maintenance programme
- A clearly defined and documented Maintenance Report (including recommendations) agreed and 'signed-off' by an appropriate senior manager.
- A clearly defined and documented BCM Maintenance Report Action Plan agreed and 'signed-off' by an appropriate senior manager.
- Effective and current BCPs, strategies and solutions

8. Review

The frequency of a BCM Maintenance Programme is dependent upon the nature, scale and pace of business change.

Maintenance is likely to be required when:

- There is a major change in business processes, locations or technology.
- After an exercise or test
- After an audit recommending improvements
- In accordance with the schedule defined in the BC Plan Maintenance Chapter/ Section.

5.4 REVIEWING BCM ARRANGEMENTS

Ref: BS 25999-1 Section 9.5

1. Introduction

The review activity includes

- Audit, both internal and external
- self assessment

An audit function is one of impartial review against defined standards and policies and to provide remedial recommendations. However the nature of BCM may require a different audit approach because standards are evolving. Auditing is designed to verify that the process has been followed correctly not that the solutions adopted are necessarily correct.

2. Precursors

The Audit should be conducted against a BCM Policy and appropriate standards identified by it.

3. Purpose

The purpose of a BCM audit is to scrutinise an organisation's existing BCM competence and capability; verify them against predefined standards and criteria and deliver a structured audit opinion report.

In addition the BCM function itself should periodically be subject to an Assurance process.

4. Concepts and assumptions

This approach assumes that if the process is correct and properly applied then the outcome should provide an effective and fit-for-purpose BCM competence and capability.

It is assumed that the available standards provide a suitable framework for audit. These include:

- National and international standards e.g. BS 25999-1 Code of Practice and BS25999-2 Specification (not yet published)
- Regulatory requirements e.g. The appropriate local Financial Services Authority
- Legislative requirements e.g. the UK Civil Contingencies Act (2004)
- Industry 'Good Practice' guidelines (such as this document) or those specific to the organisation's sector
- Industry standards e.g. ISO 17799 (IT Security).

5. Process

The BCM audit, like BC planning, implementation and maintenance is concerned with a complex process and requires interaction with a wide range of managerial and operational roles from both a business and technical perspective.

The BCM audit process includes:

- A BCM audit plan - which should include:
 - Identification of the type of audit to be carried out e.g. compliance, project
 - Management/control, feasibility study, due diligence or investigative.
 - Identification of the audit objectives i.e. outcomes and deliverables. The audit
 - Objectives may in part be driven and governed or restricted by legal or
 - Regulatory requirements. This includes key issues of high priority.
 - Identification of the standard audit framework (where appropriate) to be used
 - E.g. BS 25999. The audit framework may be governed or restricted by legal or

regulatory requirements.

- Definition of the audit scope:
 - Determine the corporate governance, compliance or other issues to be audited.
 - Determine the area/department/site of the organisation to be audited.
- Definition of the audit approach:
 - The auditing activities that will be undertaken e.g. questionnaires/face-to-face interview/document review/solution review.
 - Activity timetable and due dates
 - Identification of the audit evaluation criteria (standards).
 - Determine the requirement for specific subject expertise or third party assistance to conduct the audit.
- Review and information gathering via the BCM audit activities.
- Compiling and summarising interview notes, questionnaires and other sources.
- Identifying gaps in content and level of information gathered and conduct further or follow up interviews as appropriate.
- Obtaining and comparing relevant documentation e.g. Business Impact Analysis with interview data and other sources e.g. walkthrough, physical inspection, sampling).
- Reference to secondary sources e.g. standards, regulations, and 'good practice' guidelines to validate preliminary findings.
- Forming of an opinion that should reflect both the interests of the audit sponsor and the 'yardstick' set by external sources e.g. regulatory, legal, industry standard.
 - Assigning a risk weighting to individual audit item to distinguish between critical, high, medium and low risk findings.
 - Defining criteria for rating factual findings by using a clearly differentiated categorised predefined rating level.
- Providing a draft audit opinion report for discussion with key stakeholders.
- Providing an agreed audit opinion report incorporating recommendations as well as audited responses where differences of opinion persist.
- Providing an agreed remedial action plan including timescales to implement the agreed recommendations of the audit report. This should also form a key element of the BCM Maintenance Programme.
- Providing a monitoring process (in addition to the BCM Maintenance Programme) to ensure that the audit action plan to address material deficiencies is implemented within the agreed timescale.

The BCM Assurance process includes:

- Defining role accountabilities, responsibilities and authority
- Defining Key Performance Indicators (KPIs) - Objectives, measurement targets and standards
- Defining success factors
- Incorporating Key Performance Indicators in internal and external contract terms and annual appraisal
- Evaluating and reviewing performance against Key Performance Indicators, objectives, targets and defined industry standards.
- Providing a remedial action plan.

6. Methods and Techniques

The methods used for Audit should be determined by those undertaking the audit.

Self-assessment, or 'Performance Monitoring' carried out within the BCM programme itself may use performance indicators such as:

- Number of months since last active exercise.
- Number of open-issues still outstanding since last exercise.
- Completeness of the BC plan documentation.
- Number of months since last business impact analysis.
- Number of open-issues still outstanding since last business impact analysis.
- New IT application assessed for inclusion in BC Management/Plans.
- New or changed business process assessed for inclusion in BC Management/Plans.
- Adequacy/viability of Recovery Team dynamic data such as team members, contact telephone numbers, notification/supplier list, recovery site workstation allocation.
- Creation of a BCM Budget for implementation and maintenance.
- Budgetary control.
- Self assessment assurance scorecard

Qualitative assessment may come from:

- Document analysis and review.
- Interviews with staff and key stakeholders

7. Outcomes and Deliverables

The outcomes of a BCM audit include:

- An independent BCM audit opinion report that is agreed and 'signed-off' by senior management.
- A remedial action plan (s) that is agreed and 'signed-off' by the senior management
- The outcome of an unfavourable performance rating will be:
 - Acceptance of the BC Plans by the Internal Audit department as 'inadequate'.
 - The initiation of a BC review conducted by a BC professional to assist the team in improving their position.

An outcome of a self-assessment process may be:

- Improvement in the management of the BCM programme

8. Review

The policy concerning the frequency of audit should be clearly defined and documented within the organisations 'Audit Policy and Standards'.

END OF SECTION 5 - EXERCISING, MAINTAINING & REVIEWING BCM ARRANGEMENTS



BUSINESS CONTINUITY
INSTITUTE

GOOD PRACTICE GUIDELINES
2008

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

SECTION 6
EMBEDDING BCM IN THE
ORGANISATION'S CULTURE

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. 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 and 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

At the end of each section there is a summary of "Key BCM Indicators" that will support future use of the BCI Benchmarking Tool, BCI E-Learning and BCI Entrance Examinations.

The view presented in these Guidelines attempts to provide 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.

Before referencing this Section of the Guide, you are advised to read Section 1, which explains in more detail how the guide works and how to use it most effectively.

3. About Section 6 - Embedding BCM in Organisation Culture

Business Continuity Management 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.

To be successful BCM has to be taken for granted as part of normal business management, regardless of size or sector. At all points in the BCM process, opportunities exist to introduce

and enhance an organisation's BCM culture.

GUIDELINES STAGE 6:
EMBEDDING BCM IN THE ORGANISATION'S CULTURE

COMPONENTS

6.0 EMBEDDING BCM IN THE ORGANISATION'S CULTURE	1
6.1 ASSESSING THE LEVEL OF BCM AWARENESS & TRAINING	1
6.2 DEVELOPING BCM WITHIN THE ORGANISATION'S CULTURE	9
6.3 MONITORING CULTURAL CHANGE	13
APPENDIX - Professional Skills Mapping	15

6.0 EMBEDDING BCM IN THE ORGANISATION'S CULTURE

Ref: BS 25999-1 Section 10 & BS 25999-2 Section 3.3

1. General Principles

The successful establishment of a Business Continuity Management (BCM) within the organisation's culture is dependent upon its integration with the organisation's strategic, and day-to-day, management and alignment with its business priorities.

A BCM culture will ensure that an organisation can:

- Develop a BCM programme more efficiently
- Instill confidence in its stakeholders, especially staff and customers, in its ability to handle disruptions
- Increase its resilience over time by ensuring BCM implications are considered in decisions at all levels
- Minimise the impact and likelihood of disruptions

The process for sustainable developing and embedding BCM in the organisation's culture is a regular iteration of the following three steps:

- Assessing the current level of awareness of, and commitment to, BCM against the desired level; thus identifying the 'training gap' that exists between the two
- Designing and delivering a campaign to create corporate awareness and develop the skills, knowledge and commitment required to ensure successful Business Continuity Management.
- Checking that the awareness campaign has achieved the desired results, and monitoring BCM awareness in the longer term

There is a limit to which any programme can alter the culture of an organisation; and attempts to change attitudes may have unexpected effects which may be the opposite of those intended.

Factors for success include:

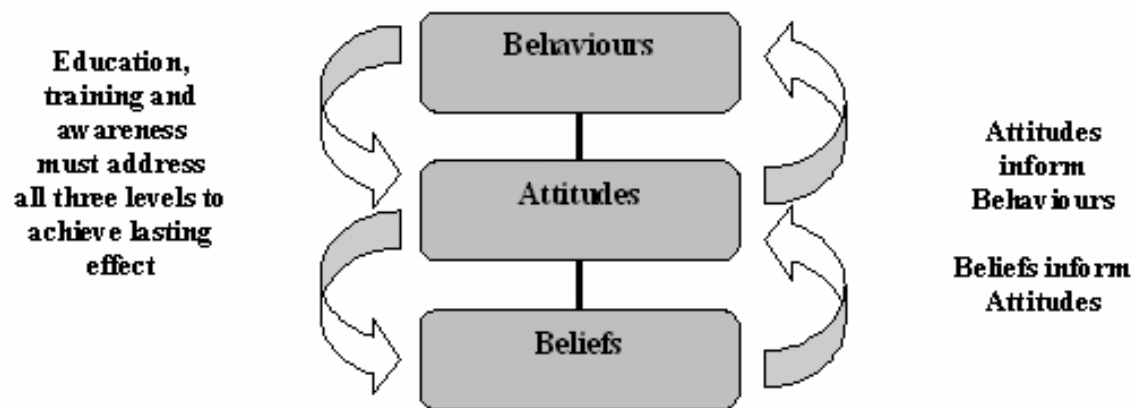
- Visible and continued support by senior management. This must include adequate budget to support the awareness campaign over time. It is also important to gain commitment from managers and operational staff who are required to implement Business Continuity Management.
- Consultation, with everyone involved with BCM, in developing the campaign. As well as providing focus for the awareness effort, consultation in itself helps raise awareness and may help prepare the way for commitment to new working practices.
- Focus on the business priorities of the organisation. Relating the campaign message to corporate and individual WIIFM ("What's In It For Me?") factors helps to provide justification for BCM and working practices that support it.

The awareness campaign and its messages should be tailored to target audiences. These audiences are both internal, for example BCM practitioners and general staff - and external, for example key stakeholders and third parties that are dependent on (or may adversely affect) the organisation's own business continuity management effort. External awareness is particularly important where BCM operates in an outsourced environment.

Organisational culture is manifested in shared values, operating norms, styles and patterns of behaviour. It is frequently described as 'the way we do things around here' or 'what you have to do to get on'.

Experience has shown that behavioural change initiatives fail to attract lasting commitment

unless attitudes and beliefs are also engaged. One specific belief 'It will never happen to me' is a particular barrier to BCM. In order to really change behaviours, it is necessary to influence the attitudes. In order to influence attitudes, it is necessary to develop and establish beliefs. Thus, achieving cultural change can be a subtle and lengthy process.



This stage describes the process of assessing and increasing BCM awareness and training within the organisation and therefore differs in structure to BS 25999-1 section 10 which is focussed on defining the outcomes of that process.

6.1 ASSESSING THE LEVEL OF BCM AWARENESS & TRAINING

1. Introduction

Before planning, and designing the components of, an awareness campaign, it is important to understand what level of awareness currently exists, and what level is desired following the delivery of education, training and awareness. It is also important to identify how the desired level of awareness will be measured and what changes will manifest the new BCM culture.

The organisation's level of awareness will be constantly changing as personnel join and leave. Internal and external events may also lead to a sudden increase in awareness and knowledge of BCM issues though these often fade quickly so the BCM programme should be ready to seize on and develop these opportunities when they arise.

Consideration should be given to extending the scope of the BCM awareness programme to the organisation's suppliers, customers, contractors and other stakeholders.

2. Precursors

The BCM Policy provides the framework for supporting the need and requirement for cultural change.

3. Purpose

The purpose of this activity is to assess current and desired levels of BCM awareness, define what areas the awareness campaign must target and how the campaign can most effectively be run.

4. Concepts and Assumptions

An audit of current BCM awareness should seek to establish the level of knowledge of, and commitment to BCM. Evidence will be found chiefly in behaviours, but there are other sources within the organisation.

Those involved in making the awareness assessment should have a good understanding of the business and its BCM aims. They should also have, or be able to call on those with, an appropriate level of competency in education, training and awareness activities, and suitable diagnostic and interpersonal skills.

As for other stages in the awareness campaign, this activity requires consultation with, and the co-operation of, staff throughout the organisation, from senior management through BCM practitioners to staff without specific BCM roles, but a general responsibility to "play their part" in BCM. In particular, senior management should, from the outset, provide support for the awareness work, both in terms of material resource and commitment to the mission.

5. Process

The awareness assessment activity is effectively a Training Needs Analysis ("TNA") and comprises three principal tasks:

1. Establishing the current level of awareness of BCM
2. Specifying the desired level of awareness or training, and how this will be measured
3. Identifying the nature and scope of the "Training Gap" to be bridged by the campaign

Requirements

Specific skill requirements for BCM staff include:

- Programme management

- Business impact analysis
- Developing and implementing BC plans
- Running an exercise programme

More general education in BCM issues should be identified for BCM staff involved in programme for example to:

- Understand trends and new developments in the subject
- Explore the possibilities and issues of new technologies
- Learn how other organisations are addressing similar challenges

For other BCM-related roles specific skills for incident response may be required such as:

- Fire evacuation
- Damage limitation
- Salvage and damage assessment
- Equipment restoration
- Leadership

General staff awareness requirements may include:

- How to raise the alarm
- Responding to specific threats
- What to do when evacuated from the site
- Knowledge of recovery plans
- Integration of basic awareness into staff initiation training

6. Methods and Techniques

Establishing the current level of awareness of BCM

This activity is an information gathering exercise. The objective should be to establish statistical indicators of any gaps in awareness, and an assessment of the appreciation of, and commitment to, BCM in target groups of staff.

Sources should include:

- Documentation: including corporate policy statements and procedures, incident and crisis response reports, accounts of previous BCM tests and exercises, relevant IT system and business metrics
- People Feedback: including interviews with senior management and business managers, focus groups with practitioners and end-users
- Observation: including on-the-job reviews of current working practices (for example, in comparison with corporate policy)

Specifying the desired level of awareness, and how this will be measured

This activity is about specifying the behaviours and related performance indicators that will confirm to the business a satisfactory level of BCM awareness in each staff target group. This specification should be agreed with senior management (in terms of corporate performance on BCM) and with managers and BCM practitioners (in terms of the feasibility and integration with working practices).

The specification will depend on the nature and scope of the business, its BCM requirements and effort, but may include the following:

- Specific skills required for BCM response to disruptions
- Enhanced working practices that support BCM developments
- A better understanding of, and material support for, BCM issues by staff generally
- A higher BCM profile in corporate decision-making, policy and culture

Identifying the nature and scope of the "Training Gap" to be bridged by the campaign

This activity requires the comparison of the results of steps 1 and 2 described above. The nature and scope of the Training Gap should be identified both in terms of the BCM subjects to be addressed by the campaign, and which delivery type - education (information), training (skills) or awareness (appreciation of, and commitment to, BCM) - is most effective.

The awareness of staff may be defined at one of four levels:

- Unconscious Incompetence is defined as the condition in which staff are unaware of BCM issues. They do not know what they don't know.
- Conscious Incompetence is defined as the condition in which staff are aware of BCM generally, but know little about its detailed requirements.
- Conscious Competence is defined as the condition in which staff are cognisant of the BCM issue and are proficient (e.g. In following documented procedures) in supporting BCM
- Unconscious Competence is defined as the condition in which staff are fully competent in applying BCM in a variety of circumstances.

7. Outcomes and Deliverables

The outcomes from the awareness assessment should include:

- A statement of the current level of awareness and effectiveness of staff to support BCM
- A statement of the desired level of awareness and how this will be measured
- A definition of the Training Gap, including BCM subjects that require greater awareness, staff attitudes to BCM - since this will help define the overall message of the awareness campaign - and the level (s) of competence found in each target group.

8. Review

The awareness assessment should be carried out at the start of the awareness campaign, again following the main thrust of the campaign, and periodically thereafter as a monitoring capability.

Additionally, awareness assessments may be needed in response to changes in:

- Organisational business processes that affect BCM priorities
- Legislation affecting BCM requirements
- The BCM risks including security threats and vulnerabilities and other business-related risks
- Corporate and client/partner requirements for the availability of information and services, including accepted industry Best Practice e.g. BS25999 and ISO27001

6.2 DEVELOPING BCM WITHIN THE ORGANISATION'S CULTURE

1. Introduction

The activities available to influence culture include:

- Training - specific BCM related skills
- Education - general BCM knowledge
- Awareness - specific knowledge for BCM issues

Designing and delivering these comprises three principal activities:

- Design
- Delivery Planning
- Delivery

2. Precursors

The BCM Policy provides the framework for supporting the need and requirement for cultural change. Within the BCM culture and awareness activity, the design and delivery of education, training and awareness must be derived from an accountable Training Needs Analysis (see previous step).

The responsibilities of individuals within the BCM programme need to be assigned before the programme is designed.

3. Purpose

The purpose of this activity is to define the BCM messages to be assimilated by staff, and select the most effective means to deliver those messages.

4. Concepts and Assumptions

Education, training and awareness can be delivered in many ways; it is critical to the success of an awareness campaign that the most appropriate and effective methods of delivery are selected.

The planning and design of the campaign should be hierarchical, starting with objectives derived from the definition of the Training Gap and its constituent features. Teaching points should in turn be identified from the specific knowledge, skills and awareness items that need to be assimilated by staff to bridge the Gap.

Staff with no particular responsibility for BCM may need to attain only awareness, or a prescribed level of proficiency, in carrying out those BCM-related tasks that are part of the role within the organisation. BCM practitioners, however, should receive a structured training path that delivers knowledge, skill and finally includes competency in BCM via opportunities to put their skills into practice.

The campaign must be costed and the effort required agreed by senior management at an early stage in the process. The availability of staff to attend training events should also be taken into account when planning the strategy and the campaign timetable.

5. Process

Designing and delivering education, training and awareness comprises three principal activities:

- Design
- Planning
- Delivery

Design

The overall design may consider first raising awareness of the BCM issue generally, to create an appetite for formal training or similar events where the key information will be delivered.

Following formal learning events, further information and opportunities for learning should be provided through, for example, corporate newsletter pages and Intranet sites, discussion groups and other activities.

In designing the campaign, the following key tasks should be completed:

- Identify the audiences for awareness, and the key education, training and awareness ("ET&A") issues to be delivered
- Prioritise the teaching points that comprise the BCM ET&A issues
- Select the order and delivery methods required for the prioritised teaching points

Delivery Planning

The term "campaign" has been used throughout, for emphasis: the achievement of cultural change will require a long term, campaigning approach. The delivery planning task should consider the most cost-effective forms of delivery and take into account staff availability and working practices. This task should also consider publicising the campaign itself as part of the awareness drive.

Key activities in this task should include:

- Discussion and agreement of the proposed campaign by Senior Management
- Piloting key elements of the campaign with a selection of business managers and staff focus groups and defining success criteria
- Planning for integration of the BCM message with induction and refresher training, and its inclusion in other staff training
- Pilot runs and assessments of proposed training events

Delivery

The strategy chosen for education, training and awareness depends on individual circumstances; therefore the only the following general recommendations for an ET&A campaign can be offered:

- The campaign should raise awareness of BCM issues for the organisation and the individual employee. Senior Management support for the campaign should be evident in training literature and events.
- Formal training should only be offered when there is evidence that awareness of the issues has been accepted. The assimilation of the knowledge or skills delivered by the training should be assessed, and any shortfalls addressed.
- Following the completion of formal training events, refresher ET&A effort should be made, to ensure that staff remain aware of the continuing (and changing) needs for BCM.

6. Methods and Techniques

There are many theories about how adults learn, and a corresponding variety of delivery strategies. While BCM practitioners can supply the factual content of the training, they should consider working with training experts to develop the strategy and deliver the campaign.

It is important to recognise that awareness is not confined to formal training, and requires that the issue, in this case BCM, be integrated with working practices. Thus, opportunities should be found to include BCM "on the agenda" wherever possible. Examples are offered below.

Information resources:

- Internet BCM sites
- Books, periodicals and industry publications
- Conferences and seminars

Training resources:

- External approved training courses
- Formal academic educational programmes
- BCI Regional Forums and working groups
- Industry sector working groups
- Certification bodies
- Internal training, including specific induction and refresher courses
- Distance learning (CBT, video, reading)
- Certification bodies
- BCM and Incident Management exercises (internal or external)

Awareness resources:

- Briefing Papers
- Corporate newsletters, bulletins, articles staff magazines
- Visits to work area recovery sites and Incident management centres
- Intranet Web Sites
- Exercising, Rehearsal and Testing of the organisation's BCM plans
- Professional BCM practitioners within the organisation
- Remuneration and rewards through the performance and appraisal system
- Participation in other organisation's BCM exercises or real events
- Inclusion of BCM related objectives through the organisation's performance and appraisal mechanisms

7. Outcomes and Deliverables

The deliverables of the campaign will include a range of learning events, including live training, distance learning, awareness events and the promotion of BCM issues in working practices. Clearly, the nature and scope of these are dependant on the specific BCM awareness goals of the campaign.

The outcomes of the campaign may include:

- Higher general awareness of the need for BCM
- Create awareness of BCM risks to the organisation and of business priorities
- Identification of an acceptable approach to BCM which can be integrated into working practices
- Improved effectiveness in conducting specific BCM tasks
- More effective responses to actual business continuity incidents
- Higher demands on BCM practitioners e.g. Through increased concern about BCM by business managers

8. Review

Training should be carried out as part of staff induction and refresher training, and revised and presented in response to changes in:

- Organisational business activities that affect BCM priorities
- Legislation affecting BCM requirements
- BCM risks, including security threats and vulnerabilities and other business-related risks
- Corporate and client/partner requirements for the availability of information and services, including accepted industry Good Practice e.g. BS 25999-1 and ISO17799

6.3 MONITORING CULTURAL CHANGE

1. Introduction

Clearly, both the overall achievement of the campaign and the success or otherwise of specific components, must be reviewed in order to continuously improve the relevance and effectiveness of the work done.

Furthermore, the awareness campaign should be viewed as an ongoing task, and periodic reviews made to check awareness and identify any effort required to maintain it at an acceptable level.

2. Precursors

The BCM Policy provides the framework for supporting the need and requirement for cultural change. Within the BCM culture and awareness activity, the maintenance and improvement of education, training and awareness effort must be derived from comparison against the original objectives arising from the awareness assessment and Training Needs Analysis.

3. Purpose

The purpose of education, training and awareness assessment is to maintain the quality and effectiveness of the campaign, ensure currency with corporate, industry and other pertinent BCM issues, and ensure that the required level of BCM awareness is achieved.

4. Concepts and Assumptions

The effectiveness of education, training and awareness can be measured on a number of levels: improved performance in individuals, higher standards across the organisation, increased emphasis on BCM in the corporate culture.

As with all research, care must be taken to ask the right questions to elicit the relevant responses, to interpret data correctly, and to remain vigilant for issues outside the central training remit which may be relevant for BCM culture generally.

5. Process

- Solicit and collate feedback on specific training events. While some training events may be successful and others less so, it is important to look for the underlying trends - for example, particular modules within a training course that consistently draw criticism.
- Monitor effectiveness. While short-term feedback can provide information about campaign components and allow their improvement, the long-term effect of the campaign is more important and may be manifested in less tangible terms (for example, heightened awareness). However, the effectiveness of the campaign should be quantified wherever possible in terms of business improvement and "the bottom line".
- Periodically monitor awareness. Senior management should be prepared to budget for assessment exercises and possible subsequent action on a regular (annual) basis.

6. Methods and Techniques

Evaluation may take many forms. Effective evaluation will combine a range of short- and long-term methods, reviewing both the form and content of the campaign itself and its effect on BCM within the organisation.

Wherever possible, the evaluation results should be expressed in terms of the benefits of the campaign to the business.

Specifically, the evaluation of training courses may include discussions, quizzes or short examinations during the course to check and align teaching 'in flight'. Course Evaluation Forms

may be used to improve continuously the course structure and content. Evaluation of a course should be based on a number of runs, rather than a single instance.

7. Outcomes and Deliverables

The deliverables of the training and campaign review should include a range of reports for appropriate levels within the organisation. These should include senior management, relevant business managers and BCM practitioners and training providers.

The outcomes of the campaign assessment should be reported to staff via corporate channels, and may include:

- Identification of further education, training and awareness requirements
- Identification of professional development opportunities for BCM practitioners
- Improvements in working practices

8. Review

Evaluation of the campaign should be made both during and after the bulk of the campaign has run to allow realignment of the strategy and to review whether the campaign has achieved its overall objective of bridging the Training Gap identified in the initial awareness assessment.

A regular awareness audit should be conducted, and any shortfall addressed.

APPENDIX - Professional Skills Mapping

This is a mapping of the 10 BCI/DRII Certification Standards into the six stages of the Good Practice Guidelines to indicate which skills are required at each stage. Note that some skills are applicable to more than one stage.

1. Business Continuity Programme Management

- 1.A.1 Lead Sponsors in Defining Objectives, Policies, and Critical Success Factors
 - Scope and objectives
 - Legal and requirements reasons
 - Case histories and industry best practices
- 1.A.2. Co-ordinate and Organise/Manage the initiation of the overall BCM Process
 - Using a steering committee and project task force.
- 1.A.3 Oversee the BCM Process Through Effective Control Methods and Change Management
- 1.A.4. Present (Sell) the Process to Management and Staff
- 1.A.5 Develop Budget to initiate the process.
- 1.A.6 Define and Recommend BCM Structure and Management
- 1.A.7 Develop and implement the BCM Process

2. Understanding the organisation

- 2.A.1 Identify Knowledgeable Functional Area Representatives for the Business Impact Analysis (BIA) process.
- 2.A.2 Identify Organisation Functions including information and resource (people, technology, facilities, etc.)
- 2.A.3 Identify and Define Criticality Criteria
- 2.A.4 Obtain management approval for criteria defined
- 2.A.5 Co-ordinate Analysis
- 2.A.6 Identify Interdependencies (internal and external to the organisation)
- 2.A.7 Define Recovery Objectives and Timeframes
- 2.A.8 Define Report Format
- 2.A.9 Prepare and Present Agreed BIA to Management
- 3.A.1 Identify Potential Risks to the Organisation
 - 3.A.1.a Probability
 - 3.A.1.b Consequences/Impact/severity
- 3.A.2 Understand the Function of Risk Reduction/Mitigation Within the Organisation
- 3.A.3 Identify Outside Expertise Required
- 3.A.4 Identify Exposures
- 3.A.5 Identify Risk Reduction/Mitigation Alternatives
- 3.A.6 Confirm with Management to Determine Acceptable Risk Levels
- 3.A.7 Document and Present Findings

3. Determining BC Strategy

- 4.A.1 Understand Available Alternatives and Their Advantages, Disadvantages, and Cost Ranges, including mitigation as a recovery strategy
- 4.A.2 Identify Viable Recovery Strategies within Business Functional Areas
- 4.A.3 Consolidate Strategies
- 4.A.4 Identify Off-site Requirements and Alternative Facilities
- 4.A.5 Develop Business Unit Strategies
- 4.A.6 Obtain Commitment from Management for developed Strategies

4. Developing and Implementing a BCM Response

Incident Management Plan

- 9.A.1 Establish Programs for Proactive Crisis Communications
- 9.A.2 Establish Necessary Crisis Communication Co-ordination with External Agencies (local, state, national government, emergency responders, etc.)
- 9.A.3 Establish Essential Crisis Communications with Relevant Stakeholder Groups
- 9.A.4 Establish and Exercise Media Handling Plans for the Organisation and its Business Units

Business Continuity Plan

- 6.A.1 Identify the Components of the Planning Process
 - 6.A.1.a Planning methodology
 - 6.A.1.b Plan organisation
 - 6.A.1.c Direction of efforts
 - 6.A.1.d Staffing requirements
- 6.A.2 Control the Planning Process and Produce the Plans
- 6.A.3 Implement the Plans
- 6.A.4 Test the Plans
- 6.A.5 Maintain the Plans
- 5.A.5 Identify the Command and Control Requirements of Managing an Emergency
- 5.A.6 Recommend the Development of Command and Control Procedures to Define Roles, Authority, and Communications Processes for Managing an Emergency
- 10.A.1 Identify and establish liaison procedures for Emergency Management
- 10.A.2 Co-ordinate Emergency Management with External Agencies
- 10.A.3 Maintain current knowledge of laws and regulations concerning Emergency Management as it pertains to the own organisation
- 5.A.1 Identify Potential Types of Emergencies and the Responses Needed (e.g., fire, hazardous materials leak, medical)
- 5.A.2 Identify the Existence of Appropriate Emergency Response Procedures
- 5.A.3 Recommend the Development of Emergency Procedures where none exist
- 5.A.4 Integrate Disaster Recovery/Business Continuity/Crisis Management Procedures with Emergency Response and Escalation Procedures
- 5.A.7 Ensure Emergency Response Procedures are Integrated with Requirements of Public

Authorities (Refer also to Subject Area 10, Co-ordination With External Agencies)

5. Exercising, Maintenance and Review

- 8.A.1 Pre-plan and co-ordinate the Exercises
- 8.A.2 Facilitate the Exercises
- 8.A.3 Evaluate and Document the Exercise Results
- 8.A.4 Update the Plans
- 8.A.5 Report Results/Evaluation to Management
- 8.A.6 Co-ordinate on-going Maintenance of plans
- 8.A.7 Assist in Establishing Audit Program for the Plans

6. Embedding BCM in the Organisation's Culture

- 7.A.1 Establish Objectives and Components of Corporate BCM Awareness & Training Program
- 7.A.2 Identify Functional Awareness & Training Requirements
- 7.A.3 Develop Awareness & Training Methodology
- 7.A.4 Acquire or Develop Awareness & Training Tools
- 7.A.5 Identify External Awareness & Training Opportunities
- 7.A.6 Identify Alternative Options for Corporate Awareness & Training