The Business Continuity Institute

# GOOD PRACTICE GUIDELINES 2010

## GLOBAL EDITION

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

Business Continuity
Institute

# Contents

## BCM – Management Professional Practices

### 01 Policy and Programme Management

### 02 Embedding BCM in the Organization's Culture

# BCM – Technical Professional Practices

## 03 Understanding the Organization

## 04 Determining Business Continuity Strategy

## 05 Developing and Implementing a BCM Response

## 06 Exercising, Maintaining and Reviewing BCM

## Supporting Information

## Acknowledgments

These Guidelines draw upon the considerable academic, technical and practical experiences of the members of the Business Continuity Institute – senior practitioners who have developed and shaped the concept of Business Continuity internationally.

Good Practice Guidelines (GPG) 2010 is intended for use by practitioners, consultants, auditors and regulators with a working knowledge of the rationale for BCM and its basic principles. They are not intended to be a beginner's guide, although they do provide excellent material for those wishing to become certified BCM practitioners through the CBCI examination scheme. Newcomers to the discipline should also work alongside an experienced practitioner or attend an appropriate education programme.

Work on GPG 2010 commenced in February 2009 with the appointment of a project team with individual group leaders. The initial drafts were produced by September 2009, with peer reviews, wider consultation and assessment taking places during October and November. Final consolidated versions were agreed by the Editor in Chief during December 2009 and submitted for review and approval by the BCI Membership Council Quality Assessment Group in January 2010. Final design work, publication and launch planning took place in February and March 2010.

The project team consisted of:
Editor in Chief: **Lyndon Bird FBCI**
Chief Reviewers: **Ian Charters FBCI, Mel Gosling MBCI**
Quality Assurance Team Leader: **Lesley Grimes MBCI**
Committee Secretary: **Jan Gilbert**
Editorial Support: **Lee Glendon**
Glossary Support: **Mark Penberthy FBCI**

Practice Group Leaders: Ian Charters FBCI, Steven Cvetkovic SBCI, Mel Gosling MBCI, Angela Hobley MBCI, Odile Nectoux AMBCI, Anton Wroblewski MBCI

In addition to the above, the following BCI members and staff gave their time and intellectual rigour to conducting peer reviews, suggesting improvements and proof reading. Without their support we would have had a much less comprehensive document.

Howard Booth MBCI, Stacey Farrow MBCI, Debbie Featherstone AMBCI, Achilles Figueiredo AMBCI, Ulysses Figueiredo MBCI, Ian Griffiths MBCI, Nic Handy MBCI, Gayle Hedgecock MBCI, Mike Hill FBCI, Doug Kettle MBCI, Penny Killow MBCI, David Lightfoot MBCI, Jorge Lozano MBCI, James McAlister MBCI, Charlie Maclean-Bristol MBCI, Dominic Marino AMBCI, Margaret Millet MBCI, Sarah Morgan MBCI, Norman Powell MBCI, Marie-Hélène Primeau MBCI, Clifford Seow MBCI, Brigitte Theuma MBCI, Pauline Wilson MBCI and John Worthington MBCI.

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 agreed that they have no copyright or IP rights to the material, which remains the property of the Business Continuity Institute. The BCM Lifecycle diagram and some glossary terms are used with thanks to the British Standards Institution.

## BCI Professional Qualifications

For those individuals who wish to become professional members of the BCI, competence needs to be shown in all six professional practices. The CBCI examination will test knowledge of this GPG 2010 subject matter across all six areas. The questions are based upon the contents of this guide. Successful candidates will be awarded a pass or a pass with merit.

For those wishing to upgrade to professional practitioner levels (AMBCI, SBCI, MBCI and FBCI) proven experience will also need to be demonstrated across the professional practices. Detail of the experience needed for each level is available at **www.thebci.org**.

**Lyndon Bird FBCI**
**Editor in Chief**
**International Technical Director**
**The Business Continuity Institute**

## Introduction to the Guide

This introduction sets the context for reading the BCI Global Good Practice Guidelines 2010. The Business Continuity Management profession has changed considerably since the formation of the BCI in 1994 and will continue to develop as its application and value is recognized by a wider audience.

The timing of the publication of this Guide gives us pause for reflection: we are experiencing the first global influenza pandemic of the 21st Century. We are also experiencing a global economic crisis not experienced in the living memory of most people on this planet and are coming to terms with new global threats including energy security, mass migration, cyber crime and climate change.

Against this background of uncertainty, it is encouraging that the discipline of BCM has proven itself able to evolve but still remains relevant in the face of these major business and societal changes.

### What is Business Continuity Management?

The definition used in previous editions of the GPG is unchanged and is consistent with British Standard BS25999.

Business Continuity Management (BCM) is an holistic process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.

### Why do we have Good Practice Guidelines?

The value of the GPG for practitioners is that is considers not just “what” but also “why” and “how”, based on real-world experiences of BCM practitioners. The GPG also has the flexibility to identify future trends, challenges and issues that practitioners are still debating.

The GPG provides a baseline and common language to help the BCM profession and individual practitioners develop. It is the basis for the entry examination into the BCI, and although it is not the sole publication on all matters relating to BCM, it does provide a proven professional benchmark for academic and commercial BCM organizations to utilise.

“Business Continuity Management (BCM) is an holistic process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.”

# BCM Trends and Observations

## No longer just for big impact, low probability physical events

BCM is no longer just about dealing with the big impact, low probability events. It is becoming an essential enabler of organizational resilience as part of "business as usual", thanks primarily to its focus on identifying and protecting sources of value within an organization. The methodology is also starting to be applied to dealing with non-physical events.

## Diverse practitioner origins

With greater awareness and adoption of BCM practices around the world, the diversity of practitioner backgrounds multiplies. While veteran practitioners may share backgrounds in IT, the armed forces or the emergency services, new entrants to the profession come from management consulting, information assurance, risk and insurance, compliance and quality. Further with BCM becoming a new academic topic, we are starting to see graduate level entry into the profession and this trend is expected to increase in the future.

## What skill sets does the BCM practitioner require?

The BCM practitioner needs to demonstrate sound analytical skills, solid programme and project management skills, effective communication and influencing skills and understand investment appraisal techniques. Along with a broad functional understanding of organizations, it is essential for the BCM practitioner to understand the language, operating model and processes of the organization in which BCM is to be applied.

## BCM embedded or centralised?

During the early phases of implementing BCM into an organization, there will be need for specialist BCM professionals to manage projects, co-ordinate plan developments, organize exercises and tests and validate BCM capabilities.

In a more mature BCM organization in which these techniques are embedded at functional level, the role of the BCM manager will move to a policy setting, governance and quality assurance activity, possibly reporting to the Head of Risk Management, Audit, Compliance or Company Secretariat.

## A dedicated BCM manager is not the only model

Business Continuity Management is cross-functional by its very nature. The BCM manager has primarily a programme management and facilitator role – the plans to ensure continuity of the business are owned by the areas of the organization that need to protect key value creating processes or assets. The cost of developing and maintaining the required level of preparedness needs to be met from these groups.

Those involved in the process will therefore differ from organization to organization, reflecting each business and operating model. For example, procurement is increasingly important in BCM programmes, due to extended supply chains and increased use of outsourcing and off-shoring.

In smaller organizations, BCM is often seen as an addendum to a multitude of other disciplines including Health and Safety, Security, and IT. However, it needs to be acknowledged that this approach links BCM to a specific event or incident type, and does not suggest an enterprise-wide approach to BCM. It is also difficult for the BCM practitioner embedded within a single function to influence beyond this function. To be effective, therefore, BCM must be recognized from the outset by senior management as a business discipline owned by the business, co-ordinated and facilitated centrally.

BCM must always start at the top – for the essential reason that BCM is about what's important and time-sensitive. Conducting, for example, a Business Impact Analysis from the ground-up might deliver a distorted and unbalanced picture of what and who is critical.

## BCM in Context

### BCM is not…

BCM is not about "everything" – such an approach betrays a lack of clarity of thought. BCM is a tool to help improve organizational performance. We must avoid it becoming another corporate "tick-box" exercise. We can help ourselves in this respect by ensuring the rigorous application of BCM to protect value in an organization but use our skills and techniques to focus on that which is both important and urgent. One example is supply chain: there is no need to mandate all suppliers to have business continuity programmes as part of the procurement process; it is better to go into more detail with those who are defined as critical in the Business Impact Analysis rather than expend the same amount of internal time (and suppliers' time) in a non-discriminatory way.

### BCM is…

### BCM and Business Resilience

Business Continuity Management, as a relative newcomer to the arena of business disciplines, clearly does not exist in a vacuum and organizations naturally seek to understand where its application will bring value and how it fits with other activities supporting the same organizational goals. We also need to recognize that organizations are not starting from a blank canvass: aspects of BCM have always been present in organizations, under different names.

The vulnerabilities in the business and operating model of an organization can be considered as seven areas: Reputation, Supply Chain, Information and Communication, Sites and Facilities, People, Finance and Customers. This use of this simple model demonstrates to top management the value and integrated nature of the BCM approach – holistic, cross-functional and cross-enterprise.

The successful application of Business Continuity Management increases an organization's resilience which in turn contributes to higher corporate performance. Resilience is widely defined as the ability of an organization to absorb, respond and recover from disruptions: BCM uniquely provides the framework to understand how value is created and maintained within an organization and establishes a direct relationship to dependencies or vulnerabilities inherent in the delivery of that value.

Resilience is not fundamentally about stopping or preventing disruption happening in the first place. Reliance on risk management or security to provide comprehensive protection will inevitably generate misplaced confidence, because most BC incidents are, by their nature, largely unpredictable.

## BCM and Risk Management

In the board room, BCM is a key contributor to effective corporate governance. It is often positioned under Risk Management and allows stakeholders to ask searching questions, such as:

- The company's business and operating model
- Key value creating products and services
- Key dependencies – critical assets and processes
- How the company will respond to a loss of or threat to any of these
- What the main threats are today and on the horizon
- Evidence that the continuity plans will work in practice

Enterprise Risk Management is another discipline firmly embedded as a strategic discipline within many large organizations today. Whereas BCM has evolved from the world of IT and "disaster recovery", the Enterprise Risk Management (ERM) methodology has evolved from the world of insurance. The BCM methodology developed at a time when ERM was still in its infancy and it was therefore necessary to incorporate risk assessment within the BCM methodology. In the more developed world of today's ERM, Business Continuity Management has been seen erroneously by some as a risk treatment for very specific types of operational events – often physical in their nature and normally characterised as "big impact, low frequency".

BCM is not about identifying, assessing and reporting every conceivable risk to an organization, its markets, customers and the wider world in which it operates and it is certainly not about allocating probabilities to event occurrences. It is important to note that BCM is focused on identifying vulnerabilities within organizations, especially those linked to the underlying value they support and understanding the impact of their non-availability over time on the organization.

The GPG is ambivalent about the presence or otherwise of an ERM system within an organization. From a BCM perspective, it is important to emphasise that if a time critical product or service has been identified, then a BCM response is essential. Any other treatment would be illusory in its efficacy.

## BCM and Crisis Management

The BCM methodology has strong links with Crisis Management through the Incident Management component. In the BCM context, incidents come in different shapes and sizes and will typically invoke the BCM plan. However, very few incidents are designated 'crises'. Crisis Management is often seen as the domain of communication and PR practitioners with the BCM practitioner in a support role, if involved at all. Crisis Management is also seen as responding to non-physical as well as physical events such as financial performance and reputation damaging incidents.

The link between Crisis Management and Incident Management is that BCM considers any disruption holistically and determines how an organization will respond to the disruption, continue its activities and recover. BCM practitioners consider the media response to an incident or crisis to be an integral part of a full Business Continuity programme.

Related again to Incident Management is Emergency Planning. The difference here is that emergency planning is normally seen as the domain of "blue light services" such as police, fire, ambulance and local authorities rather than for organizations in general, where the incident team, typically, would co-ordinate with the emergency response teams.

## BCM, Standards and Compliance

Since the original concept of the GPG was launched, a number of national and international standards bodies have attempted to codify BCM through the framework of a Management Systems Standard Architecture. The most wide-spread to date has been the British Standards Institution's BS25999, although others have emerged (or are in final stages of development) from the United States, Singapore, Australia and Canada.

At the time of writing, a new international standard for BCM, ISO22301, is under development as well as a code of practice ISO22399, so it is difficult to know exactly how this will all be consolidated. The GPG does not set out to compete with ISO or national standards. From the BCI's perspective, it is self-evident that any certifiable standard requires competent and knowledgeable people to design, implement and assure the work. This GPG establishes the specific individual competences that are essential in implementing a BCM code of practice or certification scheme within an organization.

The BCI feels that adoption of BCM should be driven by the need for higher levels of organizational resilience and consequent performance rather than by regulators and legislators. However, where compliance regulations do exist for continuity of operations, then clearly BCM is a proven methodology able to demonstrate such compliance.

### What has changed from the earlier version?

The main components remain the same but there have been some refinement of language and more emphasis on global trends and issues. There are no longer any cross references to BS25999 and no implied direct correlation between GPG 2010 and BS25999, other than at the highest level expressed by the Lifecycle model.

The Good Practice Guidelines 2010 still covers the six phases of the BCM Lifecycle but now links them more directly to what are now defined as Professional Practices (PP). The six PPs are sub-divided into two Management Practices and four Technical Practices.

#### Management Practices

- Policy and Programme Management
- Embedding BCM in the Organization's Culture

#### Technical Practices

- Understanding the Organization
- Determining BCM Strategy
- Developing and Implementing a BCM Response
- Exercising, Maintaining and Reviewing

## Who Should Read this Guide?

This GPG is not only for those BCM practitioners looking for professional certification. As a body of knowledge, the GPG is used to inform BCI training courses and awareness briefings for colleagues that need to understand BCM better. These colleagues may include PR and crisis management professionals to supply chain practitioners, and human resources personnel.

BCM is not restricted to any particular industry sector; indeed, applying Standard Industrial Classification codes to the organizations represented among the BCI's membership reveals representation in all categories. Likewise, the use of the term "business" does not mean that BCM only refers to commercially-driven organizations: the state sector can readily benefit from adopting BCM practices and likewise voluntary and not-for-profit organizations.

While BCM can demonstrate healthy adoption among medium-sized and larger organizations, there is a recognized gap in adoption among smaller businesses. There is nothing inherently "corporate" about BCM; however the BCI recognizes that few small business owners have the time or resources to follow the GPG completely so simpler alternative materials, grounded in the GPG, have been produced to aid them.

## The origins of Business Continuity Management

The exact origins of Business Continuity Management are open to some debate but certainly some aspects of the story are fully established. The original commercial Disaster Recovery sites started in the United States in the late 1970's and this inevitably created the demand for third party consultancy. This consultancy was initially aimed entirely at Data Processing or MIS (as IT/ITC was then generally called) and was technical in nature.

The subject became known as Disaster Recovery Planning (DRP).

One of the initial problems faced by pioneers in this field was the difficulty in convincing Top Management of the justification for making significant investment in something which probably would never happen. This led to the concept of a Business Impact Analysis (BIA) to add more business focus to the process.

The original BIA methodologies were in place in the US by the mid 1980's and these were quickly picked up and brought to Europe (mainly the UK) and Australia. It is therefore true that the original BIA model predates the first application of wider Business Continuity. The first consultants to successfully develop a commercial set of methodologies for DRP were from the United States but these methods were soon both established and enhanced in Europe.

It is at this point that different opinions exist about how BCM gradually evolved out of DRP. The BCI view is based upon the common knowledge, experience and memory of many long established practitioners. It does not necessarily tell the full story but it is an accurate summary, which new and prospective practitioners should benefit from knowing.

The first known use of the term "Business Continuity" was made by Ron Ginn (later to become the inaugural BCI Chairman) back in 1986, after he had researched the subject in the United States and interviewed many leading practitioners. He wrote a book entitled "Continuity Planning" which postulated an application of the DRP skill-set to a much wider range of business risks and potential operational interruptions.

A UK organization called "Survive" was started in 1988 to serve the emerging need for a forum in which Disaster Recovery people could share their experiences and knowledge. This organization was later to become a commercial provider of training, events and publications but the initial vision as a networking group proved very successful. It established similar groups in a number of mainly English speaking countries. When "Survive" decided in 1991 to drop the references to DRP and re-brand itself "The Business Continuity User Group", this had a significant impact in changing external perception of the subject.

At a similar time, two of the largest US-owned Disaster Recovery companies also changed their positioning, seeing "Continuity" as a more upbeat message than "Recovery". Unfortunately this wrongly suggested that BCM was just another name for DR and possibly hindered its growth as a new discipline, especially in North America.

Another key development was the launch of the British Standard for Information Security which quickly became ISO standard ISO17799. This included in its core principles the need for Business Continuity Management, which it defined in terms of Data Availability. This added further confusion to the debate and resulted in many IT practitioners claiming that BCM was simply a sub-set of Information Security. This view held much support in those countries in which BCM had not become established at that stage, most obviously Central and Northern Europe.

In 1993 “Survive” set up a working party to look into training and certification for the business continuity professional. There was a perceived need to distinguish between the specialist skilled practitioner and the general consultant, usually from an IT background. Similar debates were taking place in the United States at around the same time which led to the formation of the Disaster Recovery Institute.

The BCI was founded in 1994 as a direct result of the recommendations from a “Survive” working party. During the development and launch of the BCI it was necessary to define the skill set in order to measure and judge the capability of those who sought recognition or qualification. Originally it was proposed that there should be 13 or 14 skills but over time these were whittled down to 10 standards of competence. These professional competence standards were developed and agreed in a cooperative effort with the US Disaster Recovery Institute (now DRII).

Towards the end of the 20th century, the idea of a holistic end-to-end approach emerged. It was now becoming obvious that there was a need to provide protection and resilience that spanned the complete business operation. Despite the perceived “over hype” of the millennium bug, the serious work done globally by major corporations did demonstrate a high level of dependence on single suppliers and single points of failure. This thinking was already encapsulated in the Business Continuity concept first proposed many years before, but it had taken well over a decade to gain wide-scale understanding. This made initiatives such as BS25999 and other national BCM standards more viable as they could be based on a solid conceptual framework.

The 21st Century saw the determination to codify Business Continuity Management and classify it as part of the family of Management Systems Standards, following a path already forged by Quality, Information Security and Environmental Services. This started with a range of guidance standards like PAS56 from the UK, NFPA1600 from the US and various handbooks from Australia and Asia. Regulatory bodies like the FSA (UK), APRA (Australia), and Federal Reserve (US) also became active in this field, particularly after the destruction of the Twin Towers in New York. At the time of publishing this document, formal national standards now exist in a number of countries and an ISO standard is expected. However, the ISO BCM standards delivery has become delayed by a desire in some countries to extend the subject boundaries to include Security and Emergency Management, and to change the discipline name to Operational Resilience. In general the BCI is not in favour of this dilution of the core BCM discipline, but supports the well intentioned aspiration that these disciplines should be better aligned.

“The 21st Century saw the determination to codify Business Continuity Management and classify it as part of the family of Management Systems Standards, following a path already forged by Quality, Information Security and Environmental Services”

## Glossary of Terms

It is recognized that many terms and definitions exist throughout the world that relate to BCM or synergic subjects like Risk Management and Emergency Planning. It would be impossible to include them all in a glossary but the BCI does attempt to keep an up to date as possible directory of such terms and their sources, which can be found at **www.thebci.org**.

Terms in this glossary apply only to the context in which they are used in GPG 2010

For the purposes of GPG 2010, the following definitions apply.

| Abbreviation | Term | Definition |
|---|---|---|
| | **Activity** | A process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products or services. |
| | **Asset** | Anything that has value to the organization. |
| | **Audit** | A systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.<br>First-party audits are conducted by the organization itself for management review and other internal purposes, and may form the basis for an organization's declaration of conformity.<br>Second-party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf.<br>Third-party audits are conducted by external, independent auditing organizations, such as those providing certification of conformity to a standard. |
| | **Auditor** | A person with competence to conduct an audit. For a BCM Audit this would normally require a person with formal BCM audit qualifications. |
| BC | **Business Continuity** | The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level. |
| BCM | **Business Continuity Management** | An holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats—if realized—might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities. |
| | **Business Continuity Management Lifecycle** | A series of business continuity activities which collectively cover all aspects and phases of the BCM program. BCI use the same Lifecycle model as BS25999. |

| Abbreviation | Term | Definition |
|---|---|---|
| BCMS | Business Continuity Management System | Part of the overall management system that implements, operates, monitors, reviews, maintains and improves business continuity. |
| BCP | Business Continuity Plan | A documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical products and services at an acceptable predefined level. |
| | Business Continuity Programme Board | Also known as a Steering Committee, this is a management group to give advice, guidance and management authorization to the BCM. |
| BCT | Business Continuity Teams | The strategic, tactical and operational teams that would respond in an incident, and who should contribute significantly to the writing and testing of the Business Continuity Plans. |
| BIA | Business Impact Analysis | The process of analyzing business functions and the effect that a business disruption might have upon them. |
| | Compliance | Fulfilment of a requirement in a Management Systems context. |
| | Consequence | See “Impact”. |
| | Continual Improvement | The process of enhancing the business continuity management system in order to achieve improvements in overall business continuity management performance consistent with the organization’s business continuity management policy. |
| CRA | Continuity Requirements Analysis | The process to collect information on the resources required to resume and continue the business activities at a level required to support the organization’s objectives and obligations. |
| | Disruption | An event that interrupts normal business functions, operations, or processes, whether anticipated (e.g. hurricane, political unrest) or unanticipated (e.g. a blackout, terror attack, technology failure, or earthquake). |
| | Document | Information and its supporting medium such as paper, magnetic, electronic or optical computer disc or image. |
| | Event | Occurrence or change of a particular set of circumstances. See also “Incident”. |
| | Exercise | A process to rehearse the roles of team members and staff, and test the recovery or continuity of an organization’s systems (e.g. technology, telephony, administration) to demonstrate business continuity competence and capability. |

| Abbreviation | Term | Definition |
|---|---|---|
| | Facility | Plant, machinery, equipment, property, buildings, vehicles, information systems, transportation facilities and other items of infrastructure or plant and related systems that have a distinct and quantifiable function or service. |
| | Hazard | See "Threat". |
| | Impact | The evaluated consequence of a particular outcome. |
| | Incident | An event that has the capacity to lead to loss of or a disruption to an organization's operations, services or functions – which, if not managed, can escalate into an emergency, crisis, or disaster. |
| | Integrity | Ensuring and safeguarding the accuracy and completeness of assets, particularly data records. |
| | Internal Audit | See "Audit" and in particular "First-Party Audit". |
| | Invocation | The declaration that an organization's BCP needs to be put into effect in order to continue to deliver key products and services. |
| | Loss | A negative consequence. |
| | Management System | A system to establish policy and objectives and to achieve those objectives e.g. ISO 9000:2005. |
| MTDL | Maximum Tolerable Data Loss | The maximum loss of information (electronic and other data) which an organization can tolerate. The age of the data could make operational recovery impossible or the value of the lost data is so substantial as to put business viability at risk. |
| MTPD | Maximum Tolerable Period of Disruption | The duration after which an organization's viability will be irreparably damaged if a product or service delivery cannot be resumed. |
| | Mitigation | The managed limitation of any negative consequence of a particular incident. |
| | Non Compliance | The failure to fulfil an agreed requirement or expectation. |
| | Objective | An overall goal, consistent with the policy that an organization sets for itself. |
| | Organization | A group of people and facilities with an arrangement of responsibilities, authorities and relationships (e.g. company, corporation, firm, enterprise, institution, charity or association). An organization can be public, private or not-for-profit. |
| PDCA | Plan, Do, Check, Act | The ISO model used as a framework in all Management Systems standards, including BCMS. |

| Abbreviation | Term | Definition |
|---|---|---|
| | Policy | The intentions and direction of an organization as formally expressed by Top Management. The BCM policy should be consistent with the overall policy of the organization and provides the basis for the business continuity objectives. |
| | Preparedness | Activities implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions. It is also often called "Readiness". |
| | Prevention | Countermeasures against specific threats that enable an organization to avoid a disruption. |
| | Procedure | A specified way to carry out an activity. Procedures should be documented. |
| | Process | A set of interrelated activities which transform inputs into outputs. |
| | Product or Service | The output from a process. Whether the product is then called a service depends upon there being a physical element to the output.<br>Service is the result of at least one activity necessarily performed at the interface between the supplier and customer, and is generally intangible. |
| | Readiness | See "Preparedness". |
| | Record | A document stating results achieved or providing evidence of activities performed. |
| RPO | Recovery Point Objective | The target set for the status and availability of data (electronic and paper) at the start of a recovery process. |
| RTO | Recovery Time Objective | The target time within which the delivery of a product or service following its disruption is to be resumed. |
| | Resilience | The ability of an organization to resist being affected by an incident. |
| | Resources | Assets, people, skills, information, technology (including plant and equipment), premises, supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objectives. |
| | Risk | The combination of the probability of an event and its consequence. BCM concentrates on "Threats" and "Impacts" rather than "Risks". |
| | Risk Acceptance | A management decision to take no action to mitigate the impact of a particular risk. |

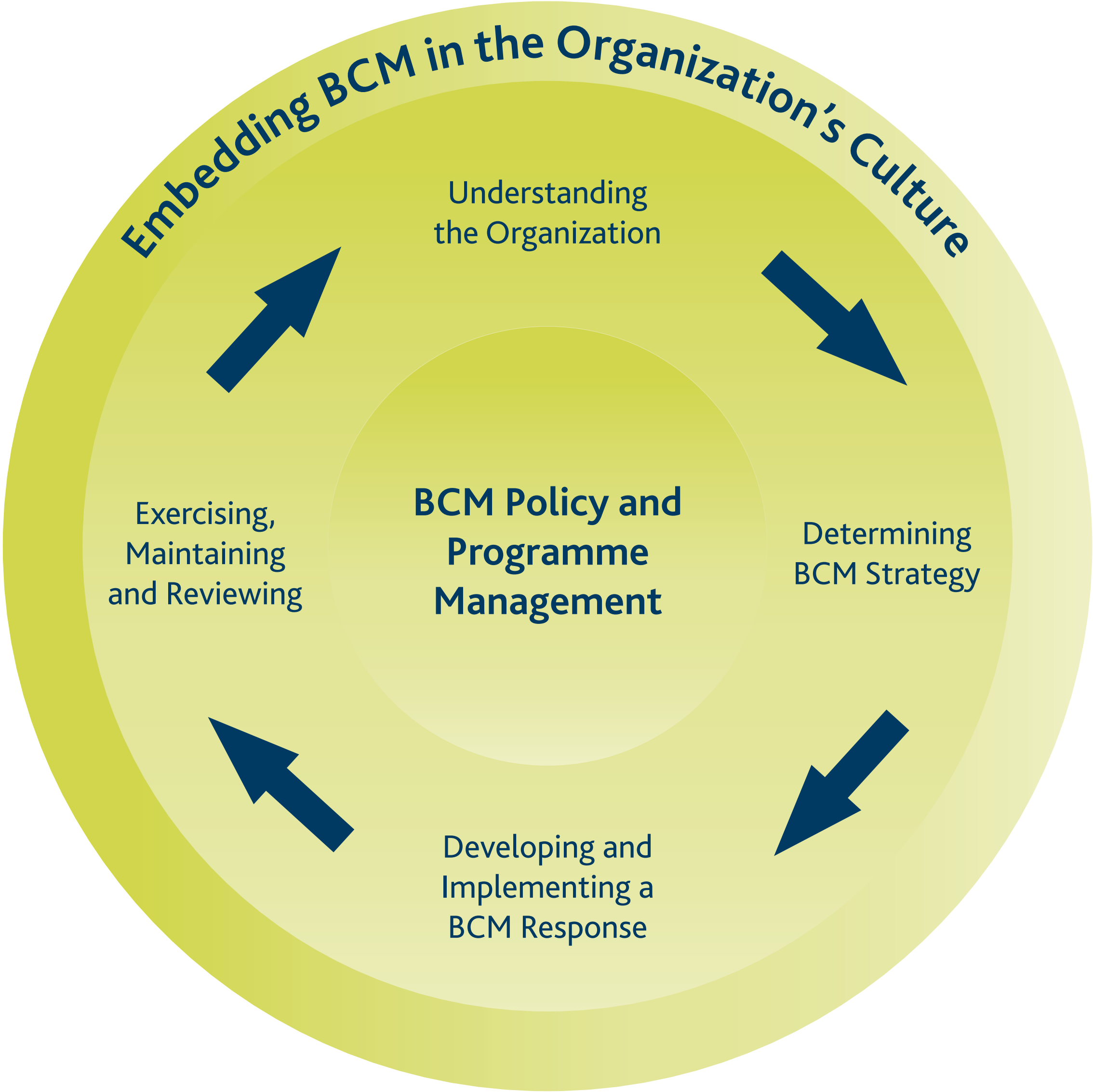
| Abbreviation | Term | Definition |
|---|---|---|
| RA | Risk Assessment | A formal but often subjective process of risk identification, risk analysis and risk evaluation. |
| RM | Risk Management | This generally includes Risk Assessment, Risk Treatment and Risk Acceptance. |
| | Risk Treatment | The selection and implementation of measures to modify risk. |
| | Stakeholder | An individual or group having an interest in the performance or success of an organization e.g. customers, partners, employees, shareholders, owners, the local community, first responders, government and regulators. |
| | Supply Chain | The linked processes that begins with the acquisition of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include suppliers, vendors, manufacturing facilities, logistics providers, internal distribution centres, distributors, wholesalers and other entities that lead to the end user. |
| | Threat | A potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community. Some threats, such as bad weather are more commonly referred to as "Hazards". |
| | Top Management | A person or group who directs and controls an organization at the highest level. In larger organizations this might be called the Board, Directors, Executives or Senior Managers. In a small organization, top management might be the owner or sole proprietor. |
| | Urgent Activity | A term used to cover activities in support of Product and Services which need to be done within a short timescale. Other terms such as immediate or time critical can also be used but "critical" alone is discouraged as it implies less urgent activities are also less important. |

GOOD PRACTICE GUIDELINES 2010

# Policy and Programme Management

01

# THE BCI Professional Practices


Embedding BCM in the Organization's Culture
Understanding the Organization
Determining BCM Strategy
Developing and Implementing a BCM Response
Exercising, Maintaining and Reviewing
BCM Policy and Programme Management

# BCM Lifecycle

# Policy and Programme Management

## Business Continuity Management Policy Overview

### Introduction

The BCM Policy is the key document that sets out the scope and governance of the BCM programme, and reflects the reasons why BCM is being implemented. It provides the context in which the required capabilities will be implemented, and identifies the principles to which the organization aspires and against which its performance can be audited.

When an organization embarks on a BCM programme it is unlikely to have a BCM Policy in place or to understand the decisions it needs to make to produce one. The key steps are:

- To develop the BCM Policy
- To align the BCM Policy with the organization's strategy, objectives and culture
- To decide upon the scope of the BCM programme

Once a BCM Policy has been agreed, a project or series of projects should be initiated to enable the organization to undertake the activities required to implement it.

In many organizations, a high level assessment of the threats to achieving the organization's strategic and operational objectives will have been undertaken as part of the business planning process. The output of this exercise can provide a useful input when setting the overall context for the BCM programme. In some regulated environments a formal Risk Assessment is a mandated activity.

# Aligning BCM Policy to Organizational Culture

## Introduction

A BCM programme needs to reflect the organization's strategy, objectives and culture to ensure that the programme is relevant, effective and appropriate.

The organization will have a culture, but this may not be well documented or articulated by Top Management. However, the organization's strategy and objectives will have been determined and agreed as part of the business planning and budgetary processes.

It is possible that some information will be market or industry sensitive and may not be visible to the BCM professional. Not having this information should not stop the BCM programme being undertaken.

## Process

The basic process used is to simply ask questions about the organization to identify its strategy, objectives and culture. These questions will include:

- What is its mission, or reason for existence?
- What are the objectives of the organization?
- How are the objectives achieved?
- What are the products and services of the organization that allow these objectives to be achieved?
- What is its direction and focus?
- What are the plans for growth, downsizing, restructuring, acquisition, or even disposal, in the short, medium and long term?
- Are new products or services being developed, and if so, what are the timescales?
- What is the geographic scale of its operations?
- What is the geographic extent of a disruption?
- What is the extent of resource loss that it wants to, or needs to, plan to survive?
- What are the current and expected market conditions in which it operates?
- Does it have competitors, and how does it compete with them?
- What is the likely reaction of customers and competitors to its operations being disrupted?
- Will competitors within the sector act to take advantage of an organization in difficulty or are they likely to support one another (which they may do to protect the reputation of the sector)?
- Does it operate in a regulated environment, and if so, what are the regulations?
- Does it have many suppliers, a few or even only one?
- What is the likely timescale within which alternative suppliers can be found?
- Does it have many customers, a few or even only one?
- Are customers prepared to pay a premium for improved reliance on delivery?

## Methods and Techniques

Two techniques can be used to identify the organization's strategy, objectives and culture:

1 Interview the Top Management team

2 Review documents produced by the organization

Key documents to be reviewed might include:

- Business plans
- Strategic plans
- Annual report
- Marketing report
- Current management information reports outlining process details, volumes, targets and, where possible, quantified value of the activity

## Review

The impact of organizational strategy on BCM 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

An alert procedure can be put in place to identify all significant organizational changes to ensure that they can be taken into account by the BCM programme. This enables BCM due diligence to be undertaken prior to a decision on the proposed change. A strategic business decision won't necessarily be abandoned because of lack of preparedness, but this limitation could impact the full economic value of the proposed change.

# BCM Programme Scope and Determining Choices

## Introduction

The purpose of setting the scope is to ensure clarity of what areas of the organization are included within the BCM programme, defined by identifying which products and services fall within it. This focuses on the key success criteria of most organizations – the delivery of products or services. An understanding of the organization's strategy, objectives and culture is required before the scope of the BCM programme can be determined and choices selected.

BCM is an iterative process, allowing an organization to initially implement BCM only in some parts of the organization, although it is anticipated that it will be extended to the whole of its operations over time. Such an approach overcomes the problems of complexity, cost and scale in implementing BCM in large organizations.

This section explains the choices available to the organization to protect its delivery of products and services, and identifies how and why it might select the various products and services of the organization for its initial implementation of BCM. These choices will define the scope of the BCM programme.

## Concepts and Assumptions

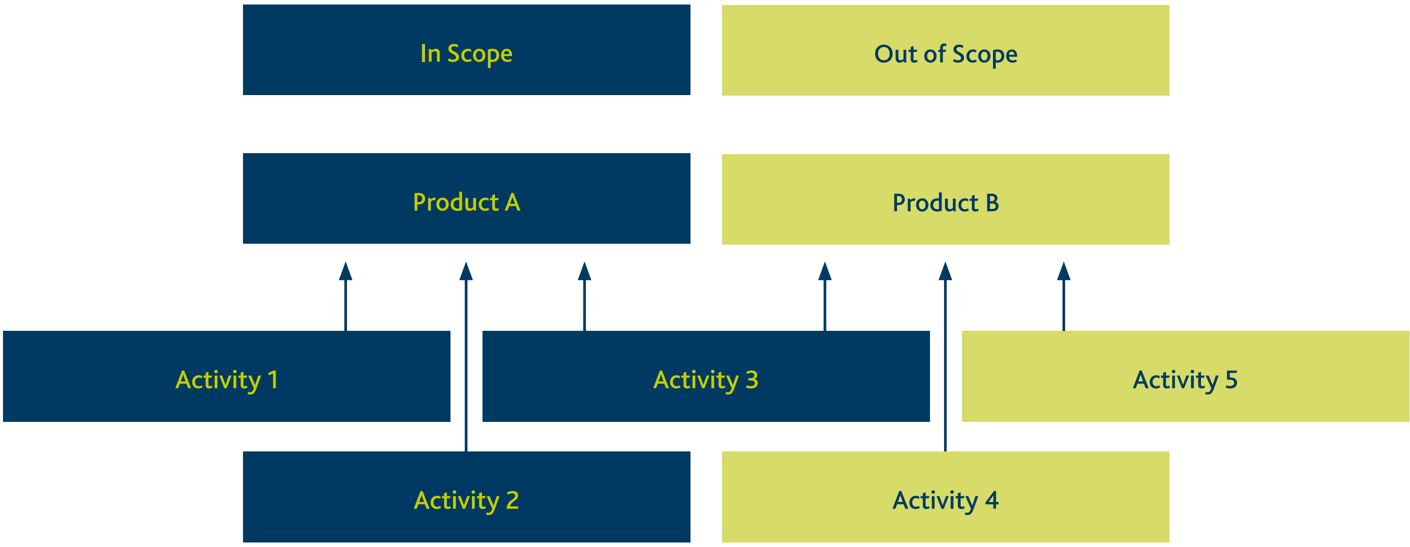
In normal practice, the decision on the scope of the BCM programme is undertaken before any other elements of the BCM Lifecycle. However, if the organization decides to undertake its initial implementation of BCM based on a perceived recovery need for a specific product or service, it might decide to conduct a high-level Business Impact Analysis to confirm the products and services to include within the initial scope (based on the impact of non-delivery).

Scope is normally limited by products and services. However location may also be used to limit scope, allowing the BCM programme to include or exclude one or more sites. It is not acceptable or 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, which allows a staged implementation of BCM across an organization. If a product or service is identified within the scope then all activities that support its delivery must be included in the BCM programme.

The documentation of 'Choices' for each product and service is intended to define how the organization intends to protect (or not) its ability to maintain their delivery, so that this decision is available for external scrutiny (for example by customers or regulators).

This is illustrated in the following diagram, where a decision has been made to include Product A in the scope of the BCM programme and exclude Product B. This means that the activities that support the delivery of Product A (Activity 1, Activity 2, and Activity 3) are In Scope, whilst the activities that do not support the delivery of Product A (Activity 4 and Activity 5) are Out of Scope.



## Process

The process requires the establishment of a BCM group that will make recommendations to Top Management

This group will review the organization's products and services against its strategy, objectives, culture, ethical policy, legal and regulatory requirements, to consider the options for each product and service. If a BIA has already been conducted to ascertain the effects of a loss of products and services the group will include the outcome of the BIA in its review.

The group will provide an evaluation report that will enable Top Management to set BCM priorities for all of its products and services.

The reasons for not including a product or service in the BCM programme, and the alternative response to loss of that product or service, need to be documented and agreed by Top Management.

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 organizational income

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

- Product or service nearing end of life (would be terminated if supply interrupted)
- Product or service with low margins (could be terminated or outsourced)

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

- The views of all key stakeholders
- Any reputation damage that may result from an interruption or termination of a product
- The relevance of any risk assessment
- Regulatory impact for regulated activities

If Business Continuity is the chosen approach for a particular product or service, then it is necessary 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.

For those products and services that are deemed out of scope, the business risk of loss or non-availability is not mitigated by complete BCM, and has to be managed by alternative means. The choices available to Top Management are:

- Acceptance – accept that it is at risk of being disrupted
- Transfer – transfer the risk of disruption to a third party
- Change, suspend or terminate the product or service

The detailed implementation of these measures generally falls within the remit of Risk Management and do not follow the full BCM full Lifecycle. However, provided the measures are agreed as an appropriate business strategy, 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 organization and any change in their processes that would be necessary to accommodate it (whether determined in advance or recognized after the event). More notes on this topic can be found in Annexe 2.

## Methods and Techniques

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

- 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, to determine the likely viability of a product following a disruption to supply

## Outcomes and Review

The outcomes are:

- An agreed strategy for the protection of each of the organization's products and services
- A scope for the BCM programme, which will be documented in the BCM Policy

A review of the organization's strategy for the protection of its products and services should be carried out at least every 12 months. However, events may prompt re-examination of the strategy, such as:

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

# Developing the BCM Policy

## Introduction

The BCM Policy of an organization provides the framework around which the BCM capability is designed and built. The organization, governance and management of the implementation of BCM are prerequisites for developing a successful BCM programme. These are set out in the BCM Policy, which is owned by Top Management.

The purpose of documenting a BCM Policy is to communicate to stakeholders the BC principles to which the organization aspires.

As the purpose of the BCM Policy is one of communication, it should be short, clear, precise and to the point. A long complicated BCM Policy will be a barrier to communication.

As a minimum, the BCM Policy will identify the following elements of the BCM programme:

- Objectives
- Scope
- Responsibilities
- Methods and standards

## Process

The process to develop a BCM Policy includes:

- 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 organization's BCM policies that could act as a benchmark
- Review and conduct a gap analysis of the organization'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 organization 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 organization's Top Management
- Publish and distribute the BCM Policy using an appropriate version control system and techniques

## Methods and Techniques

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

- Review of organization's current BCM Policy
- 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 organization 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

## Outcomes and Review

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

- The organization's definition of BCM
- A definition of the scope of the BCM programme (see earlier)
- An operational framework for the management of the organization's BCM programme
- A set of BCM principles, guidelines and minimum standards
- Clearly defined responsibilities

Whilst all organizational policies should be reviewed on an on-going basis, a formal review of the BCM Policy could be triggered by many things.

# Outsourced Activities

## Introduction

It is important that the BCM Policy also covers outsourced activities. The organization's delivery of products and services should not be disrupted by a failure of a third party supplier of goods or services which are provided either to the organization or direct to the customer on the organization's behalf. If part or all of a product or service delivery is outsourced, the responsibility for its continuity remains with the organization. Stakeholders will assume the organization 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 organization.

## Process

The processes for reviewing the Business Continuity arrangements of an outsourcing company are similar to those employed for reviewing the organization's own.

It is important that access to the following information is available for assessing:

- Tenders of prospective outsourcers
- On-going adequacy of arrangements of existing outsourcing companies

Reliability of outsourcing arrangements may be increased by:

- Pre-qualification of candidate outsourcing companies
- Specification of BCM requirements in tender documentation and contract terms
- Realistic Service Level Agreement (SLA) for use during incidents at either organization
- Involving outsourcing companies in BCM training, awareness and exercising

Documentation to support outsourcing includes:

- Mandatory parameters for selection of outsourcing companies
- Contract terms which should include the right for the organization to audit the outsourcing company
- Service Level Agreement
- Documentation of results of exercises

## Outcomes and Review

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

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.

# BCM Programme Management Overview

## Introduction

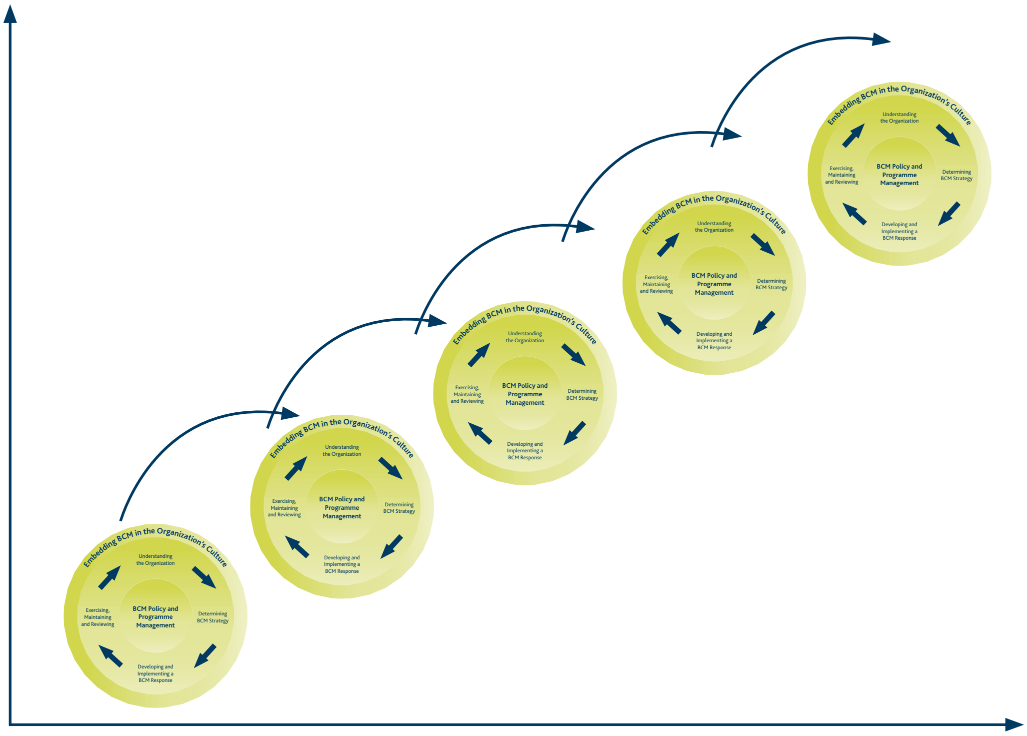
BCM is an iterative process, and needs to be actively managed. The initial aim of this stage will be to successfully complete an implementation of the BCM Lifecycle, but the long term goal of BCM programme management is to improve the organization's BCM capability, and hence its operational resilience, with successive iterations of the BCM Lifecycle, as shown in the following diagram.

The early implementations of the BCM Lifecycle will benefit from a project management approach, but as BCM matures within an organization, programme management skills are required to ensure preparedness remains current.

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

The key elements of BCM Programme Management are:

- Assigning responsibilities
- Implementing BCM in the organization
- Project management
- Ongoing business continuity management
- BCM documentation


Embedding BCM in the Organization's Culture
Understanding the Organization
Determining BCM Strategy
Developing and Implementing a BCM Response
Exercising, Maintaining and Reviewing
BCM Policy and Programme Management

Improving the Organization's BCM capability

# Assigning Responsibilities

## Introduction

A successful BCM programme is dependent upon the early identification of clearly defined roles, responsibilities and authorities to manage the BCM programme and process throughout the organization. This will have been established in the BCM Policy.

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

## Concepts and Assumptions

The BCM programme needs to be adequately resourced. This is often easier to achieve in regulated industries such as banking and financial services because many regulatory authorities consider that BCM is a cost of doing business and make it mandatory.

The response structure that will be adopted by an organization may be defined at this stage. It is often assumed that those who have developed the plans are the best individuals to respond to an incident, but the personalities required of planners and leaders are often contradictory. Any difficulties in this area should be exposed by a realistic set of plan exercises.

Those who have been involved in implementing the BCM programme may be expected to provide a lead during incident response, and BCM professionals should maintain a state of readiness so that incident management takes over smoothly if called to put plans into action. They will have the best detailed knowledge of the overall strategies and actions that need to be immediately invoked, and may need to support line management with assessment and invocation activities.

## Process

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

An individual should be appointed to manage the BCM programme and (in most organizations) will be known as the Business Continuity Manager. Depending on the size of the organization, this may be a full or part time role.

For larger organizations, additional staff may be nominated to work with the BCM Manager to assist with the following activities:

- Conduct exercises
- Information collection
- Undertake documentation revisions
- Assist in BCM implementation
- Act as BCM coordinator in their areas

Additional groups may be formed to assist in the development of the BCM programme. These include:

- **BCM Programme Board or Steering Committee** – a management group to give advice, guidance and management oversight
- **Business Continuity Teams** – the strategic, tactical and operational teams that would respond in an incident, and who should contribute significantly to the writing of the Business Continuity Plans
- **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

## Methods and Techniques

The staff appointed to the BCM programme should have the appropriate training for their role. This can be provided through using in-house or external training courses, and/or through working with external BCM professionals hired to assist with the early stages of the implementation.

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

To ensure that the BCM tasks are effective and given appropriate time and effort, the roles and responsibilities should be integrated into job descriptions and the appraisal process.

## Outcomes and Review

The roles and responsibilities within the BCM programme have been assigned to individuals who have been provided with appropriate training. These roles and responsibilities are included in their job specifications and performance objectives, and are understood by the individuals and the organization.

The level and competence of BCM staffing should be reviewed annually as part of the normal budgeting process, and may be a topic for the BCM Manager's annual appraisal and the subject of an audit.

# Implementing BCM in the Organization

## Introduction

Implementing a BCM programme involves managing a number of related projects, and the coordination of activities that balance:

- **Awareness-raising** – events which maintain the enthusiasm for undertaking a BCM programme
- **Data collection** – to determine the choice of continuity options to support the organization's objectives
- **Planning** – the development of plans to respond to incidents that might not occur
- **Mitigation measures** – the implementation of measures to mitigate the impact of an incident should it occur as the programme is being developed
- **Exercising** – exercising contingency plans

This can only be successful with adequate resources, including the assignment of roles and responsibilities to trained individuals to undertake the tasks required to implement and maintain the BCM programme.

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

## 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 organization. The only definite rule is that major decisions on continuity options and recovery strategy should not be made until the 'Understanding the Organization' 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.

## Process

The process of implementing BCM in an organization consists of:

- An initiation process
- The planning, coordination and implementation of BCM projects to undertake initial implementations of the BCM Lifecycle:
  - > Understanding the Organization (see Practice 3)
  - > Determining BCM Strategies (see Practice 4)
  - > Developing the BCM Response (see Practice 5)
  - > Exercising, Maintenance and Review (see Practice 6)
- Maintaining levels of awareness
- Ongoing management

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

- 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 organization
- Drafting a scope for the programme
- The development of a draft BCM Policy
- Data collection and continuity options selection
- Measures to mitigate specific perceived threats
- Create incident management procedures
- Identify and implement low cost quick wins

Project management disciplines should be used for the planning, coordination and implementation of BCM projects, and progress should be monitored.

During programme initiation, sufficient time should be allowed to support each activity with appropriate awareness and skills training.

## Outcomes and Review

At the end of a successful initial implementation of a BCM programme, the organization should have:

- An initial 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

In its initial implementation phase, the BCM programme should be reviewed at least monthly and on completion at defined milestones.

# Project Management

## Introduction

When undertaking an initial implementation of a BCM programme in an organization, project management disciplines should be adopted. The project management method selected should be appropriate to the size and complexity of the organization and its implementation of BCM.

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 has a clear deliverable (for example, in rolling out an awareness event across the organization).

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.

## Process

This document can be used to identify the projects required to complete an initial implementation of the BCM Lifecycle.

Each project will be planned and monitored according to the project management method chosen, and should be defined in terms of:

- Objectives
- Scope
- Tasks
- Timescales
- People involved
- Deliverables
- Milestones

Work estimates for some project stages will often depend on the outcomes of previous stages.

Project management disciplines may also be usefully applied to other 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

## Outcomes and Review

The outcome of this step is the successful delivery of the BCM Lifecycle, within agreed timescales and budgets, as part of the initial implementation of the BCM programme.

The project method adopted should include the regular review of progress on providing the deliverables against pre-defined dates for milestones, work estimates and cost.

# Ongoing Business Continuity Management

## Introduction

Once implemented, the BCM programme needs to be managed in a continuous cycle of improvement if it is to be effective. This will involve the participation of various managerial, operational, administrative and technical disciplines that need to be co-ordinated as outlined in these Guidelines.

## Concepts and Assumptions

The programme will be managed within the framework of and according to the principles contained in the organization's BCM Policy.

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

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

## Process

The Top Management of the organization should:

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

The appointed BCM person or team should (in consultation with Top Management):

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

The appointed BCM person or 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

## Methods and Techniques

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

- These Guidelines
- Assistance from external BCM practitioners
- A BCM self assessment scorecard
- Annual personnel performance contracts and appraisals
- Supplier and outsource provider relationship management
- 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 BS25999
- Internal and/or independent BCM audits
- Review and challenge

### Outcomes and Review

The outcome is a continuously improving BCM capability.

The review may include:

- A clearly defined and documented BCM programme that is agreed by the organization's Top 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 organization's BCM programme and Lifecycle
- The overview and provision of the organization's recovery strategy
- 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 in response to real incidents

An organization's BCM programme should be managed on an ongoing basis. It should be reviewed by internal or external audit on a timescale that they define.

## BCM Documentation

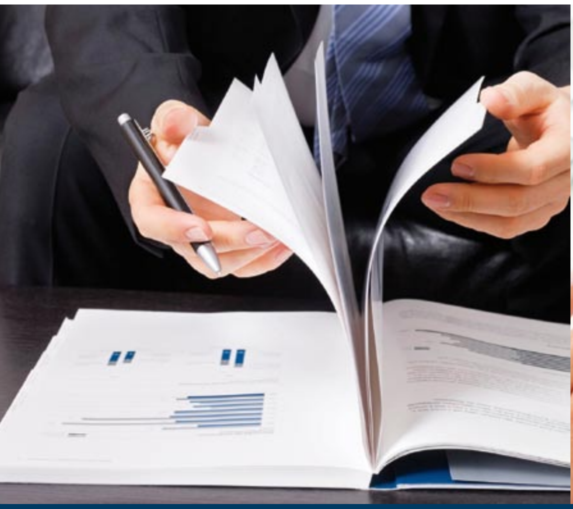
### Introduction

An important part of the BCM process is to manage the 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 organization.

Although documentation of the process is always important, it has particular significance for organizations wishing to be certified against BCM standards issued by various national or international standards authorities.

Organizations that are already certified against well established ISO management systems standards will need to review how well their BCM documentation fits with the requirement of those standards.

Organizations that intend to certify against a BCM national or international standard will need to review how their internal BCM documentation fits with the requirements of their chosen standard.



## Concepts and Assumptions

BCM documentation has three purposes:

1 To manage the BCM programme effectively
2 To demonstrate the effective management of the programme (for example, during an audit)
3 To enable a prompt and effective response to an incident

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 proprietary software or other documentation tools 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.

## Methods and Techniques

BCM documentation tools include word processing, spreadsheets, flowcharting tools, project management software and databases, or the use of specialist proprietary BCM software. It can also be used to ensure current copies of documents are available at the organization's various sites. Specialist BCM software may offer some advantages in maintenance but imposes an ongoing cost of training throughout the programme.

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

## Outcomes and Review

A current set of BCM documentation. This may include:

- BCM Policy
- BCM roles, responsibilities and resources
- Project definitions for BCM projects
- Progress reports for BCM projects
- Training and competency records for BCM personnel
- The output from a Business Impact Analysis (BIA)
- The output from a Continuity Requirements Analysis (CRA)
- Threat assessments
- BCM strategies including papers supporting the choice of the strategies adopted
- Resource level consolidation
- Incident response structure
- Incident management plans
- Business continuity plans
- Exercise programme
- Exercise 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

The review cycle for each document should be 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 as part of their audit schedule.

# Embedding BCM in the Organization's Culture

# 02

# Embedding BCM in the Organization’s Culture

## Embedding BCM in the Organization’s Culture Overview

### Introduction

The successful establishment of BCM within the organization’s culture is dependent upon its integration with the organization’s strategic and day-to-day management as well as its alignment with business priorities.

This is not unique to BCM. Other disciplines such as Quality, Health and Safety, Environmental Services, IT Service Management and Information Security have similar demands placed upon them, and consequently have used the same ISO approved management system model.

Some of the comments in this section could apply equally well to other disciplines, but wherever possible they have been presented in ways which are particularly pertinent to the BCM practitioner.

## General Principles

Organizational culture is a dynamic and evolving process which is both complex and multifaceted. It must be constantly refined and shaped, so as to enable an organization to improve its strategic alignment and performance in the environment in which it operates. If the culture is appropriate then an effective strategy can be implemented.

The established view of organizational culture is often portrayed as the combined assumptions, beliefs, values and patterns of behaviour that are shared by members of an organization. These are often not consciously understood but when taken together they create the way an organization views itself, its place in its market and the environment in which it operates.

Trying to make sense of these underlying assumptions is not straightforward. They are extremely difficult to observe with any degree of accuracy. However, it is fair to say that the 'way things are done around here' is an idea that will feature prominently in both the formal and informal organization. Hence facilitating behavioural change is very difficult to accomplish.

Having a Business Continuity Management System (BCMS) in place should ensure that an organization can:

- Manage a BCM programme efficiently
- Instil confidence in its stakeholders, especially staff and customers, in its ability to handle disruptions
- Increase its response capability over time by including BCM implications in strategic and tactical decisions at all levels
- Minimise the impact and likelihood of disruptions

These benefits are only likely to be fully realised if the culture of the organization understands the need for BCM and actively promotes its growth across the organization.

## Process

The process for sustainably developing and embedding BCM in the organization's culture is a regular iteration of the following:

- Assessment of current organizational culture
- Understanding where the organization wants to go
- Assessment and identification of the differences between the two

This will include:

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

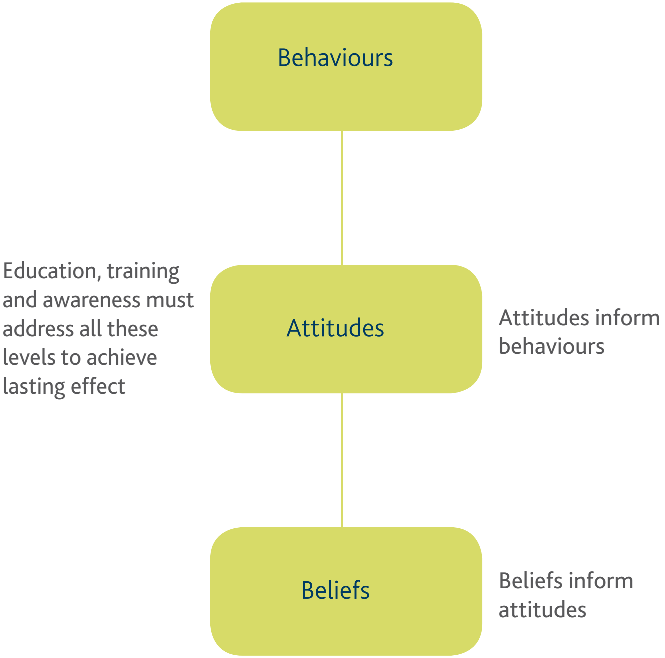
## Methods and Techniques

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 organization's own BCM effort). External awareness is particularly important where BCM operates in an outsourced environment.

The established view of organizational culture sees strategic change being constrained by rigid behavioural patterns, which are underpinned by strong social controls to predicate behaviour and is manifested in shared values, working 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 here’ is a particular barrier to BCM. In order to really change behaviours, it is necessary to influence 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.



Behaviours

Education, training and awareness must address all these levels to achieve lasting effect

Attitudes

Attitudes inform behaviours

Beliefs

Beliefs inform attitudes

Ultimately the success of embedding a BCM culture will be determined by the extent to which individuals change their behaviour, attitudes and beliefs. However because people are frequently unaware of their cultural judgements and the assumptions underpinning their ways of doing things, once corporate culture becomes established, it is relatively resistant to strategic change – hence the need for a continual iterative process to assess and challenge assumptions and practices.

## Outcomes

There is a limit to which any programme can influence and alter the culture of an organization. Attempts to change attitudes may have unexpected effects which may be counter-productive or even the direct opposite of those intended.

Implementing a BCM culture programme should not be underestimated, for it involves influencing values, beliefs and behaviours, and is a major change management challenge that requires not only education, training, awareness and participation, but strong leadership skills from key individuals.

The assessments need to be carefully considered because the analysis is rarely fully objective: people bring a whole host of prior assumptions, received wisdoms, traditional ways about doing things, inherited perceptions of the world in which they live and their position or status within it.

Factors for success include:

- Visible and continued support by Top Management. This must include adequate budget to support the awareness campaign over time. It is also important to gain commitment from middle management and operational staff who are required to implement a BCM programme
- 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 organization by relating the campaign message to corporate and individual factors

# Assessing the Level of BCM Awareness and Training

## Introduction

The BCM Policy provides the framework, which supports the need for cultural change.

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. It is also important to identify how the desired level of awareness will be measured and what changes will be manifested in the new BCM culture.

BCM competence and capability must be appropriate to the nature, scale and complexity of an organization, thus reflecting its culture and support of the business objectives.

The organization’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. As these often fade quickly, the BCM programme should be ready to seize on and develop opportunities when they arise.

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

## 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 mainly in behaviour patterns, but there are other sources within the organization. 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 analysis and interpersonal skills.

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

## Skills and Training Requirements

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

Specific skill or project requirements for BCM staff include:

- Programme Management
- Business Impact Analysis
- Developing and implementing Business Continuity plans
- Running an exercise programme

More general education in BCM issues should be provided for BCM staff involved in the programme. For example to:

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

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

- Fire evacuation
- Damage assessment
- Salvage
- 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
- Where to find information in the company about BCM

## Process

### 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 policies 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 Top 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 Top 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 awareness campaign

This activity requires the comparison of the results of the steps 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) would be most effective.

## Outcomes and Review

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 staff awareness of BCM – since this will help define the overall message of the awareness campaign – and the level (s) of competence found in each target group

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

1 'Unconscious Incompetence' where staff are unaware of BCM issues. They do not know what they don't know

2 'Conscious Incompetence' where staff are aware of BCM generally, but know little about its detailed requirements

3 'Conscious Competence' where staff are cognisant of the BCM issue and are proficient (e.g. In following documented procedures) in supporting BCM

4 'Unconscious Competence' where staff are instinctively fully competent in applying BCM in a variety of circumstances

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 such as:

- Business processes that affect BCM priorities
- Legislation or regulation affecting BCM requirements
- Increased security threats and vulnerabilities
- Corporate and client/partner requirements for the availability of information and services, including compliance with relevant standards

# Developing BCM within the Organization's Culture

## Introduction

The BCM Policy provides the framework for supporting the requirement for cultural change. Within the BCM culture and awareness activity, the design and delivery of education, training and awareness must be derived from a justifiable Training Gap Analysis. The responsibilities of individuals within the BCM programme need to be assigned before the programme is designed. 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.

The techniques which might be used include:

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

Issues to be covered for these activities include:

- Design
- Planning
- Delivery

## 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. Learning 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 organization. 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 Top 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.

## Process

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

1 Design
2 Planning
3 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, intranet sites, discussion groups and other activities. In designing the campaign, the following key tasks should be completed:

- Identify the audiences
- Identify the Education, Training and Awareness issues to be delivered
- Prioritise the teaching points that comprise the BCM Education, Training and Awareness issues
- Select the order and delivery methods required for the prioritised teaching points

### Planning

The 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 Top 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 only the following general recommendations for an Education, Training and Awareness campaign can be offered:

- The campaign should raise awareness of BCM issues for the organization and the individual employee
- Top 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 Education, Training and Awareness effort should be made, to ensure that staff remain aware of the continuing (and changing) needs for BCM

A budget must be made available for regular formal staff training and continued development of BCM qualified staff.

## 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 work with training experts to develop the strategy and to deliver the campaign.

It is important to recognize that awareness is not confined to formal training, and requires that BCM be integrated with working practices. Thus, opportunities should be found to include BCM on the agenda wherever possible.

Information resources could include:

- BCM websites
- 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 (compulsory basic training video, reading)
- 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 organization's BCM plans
- Professional BCM practitioners within the organization
- Remuneration and rewards through the performance and appraisal system
- Participation in other organization's BCM exercises or real events
- Inclusion of BCM related objectives through the organization's performance and appraisal mechanisms

## Outcomes

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 dependent on the specific BCM awareness goals of the campaign.

The outcomes of the campaign may include:

- Higher general awareness of the need for BCM
- Awareness of the importance of BCM to the organization and its 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

# Monitoring Cultural Change

## Introduction

The purpose of education, training and awareness monitoring 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.

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.

## 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 organization, and increased emphasis on BCM in the corporate culture.

Care must be taken to ask the right questions not only from an organizational perspective but also from the individual’s perspective to elicit the relevant responses, to interpret data correctly, and to remain vigilant for issues outside the central training remit that may be relevant for BCM culture generally.

The reasoning behind this is that responses are often unique and situational and so only through methods such as semi-structured interviews, participant observation and focus groups can the complexities of context and significance of people’s understanding be evaluated. BCM practitioners are likely to need assistance from learning specialists in this field.

### 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. Short-term feedback can provide information about components of a campaign and will allow their improvement, but the long-term effect of the campaign is more important and may be manifested in less tangible terms (for example, heightened awareness). The effectiveness of the campaign should be quantified, wherever possible, in terms of business improvement
- Periodically monitor awareness. Top Management should be prepared to budget for assessment exercises and possible subsequent action on a regular basis

## 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 organization.

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 the course structure, content and delivery. Evaluation of a course should be based on a number of runs, rather than a single instance.

## Outcomes and Review

The review should include a range of reports for appropriate levels within the organization. These should include Top Management, relevant business managers, BCM practitioners and training providers.

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.

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

A regular awareness audit should be conducted so that shortfalls can be identified and addressed.

# Achieving Cultural Change Through Management Systems Standards

## Introduction

Although the implementation of a formal Business Continuity Management System (BCMS) does not in itself result in cultural change, it does provide some of the pre-requisites for success. These are:

- Top Management commitment
- A formal process for performance measurement
- The need to demonstrate how well BCM has been embedded
- Assurance of the quality and accuracy of documentation
- Assurance of mandatory processes and procedures
- The involvement of a wide range of individuals at all levels
- Training needs and appropriate budgets to be established

## Management Systems

A management system for BCM can be defined as that part of the overall management system (of the organization) 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

A BCMS uses the Plan-Do-Check-Act (PDCA) cycle which is common to all ISO management systems.

| | |
|---|---|
| Plan | Establish the policy, objectives and scope of the programme |
| Do | Implement the BCM programme |
| Check | Internal audit and management review of the BCMS |
| Act | Implement the results of the review |

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

## Certification

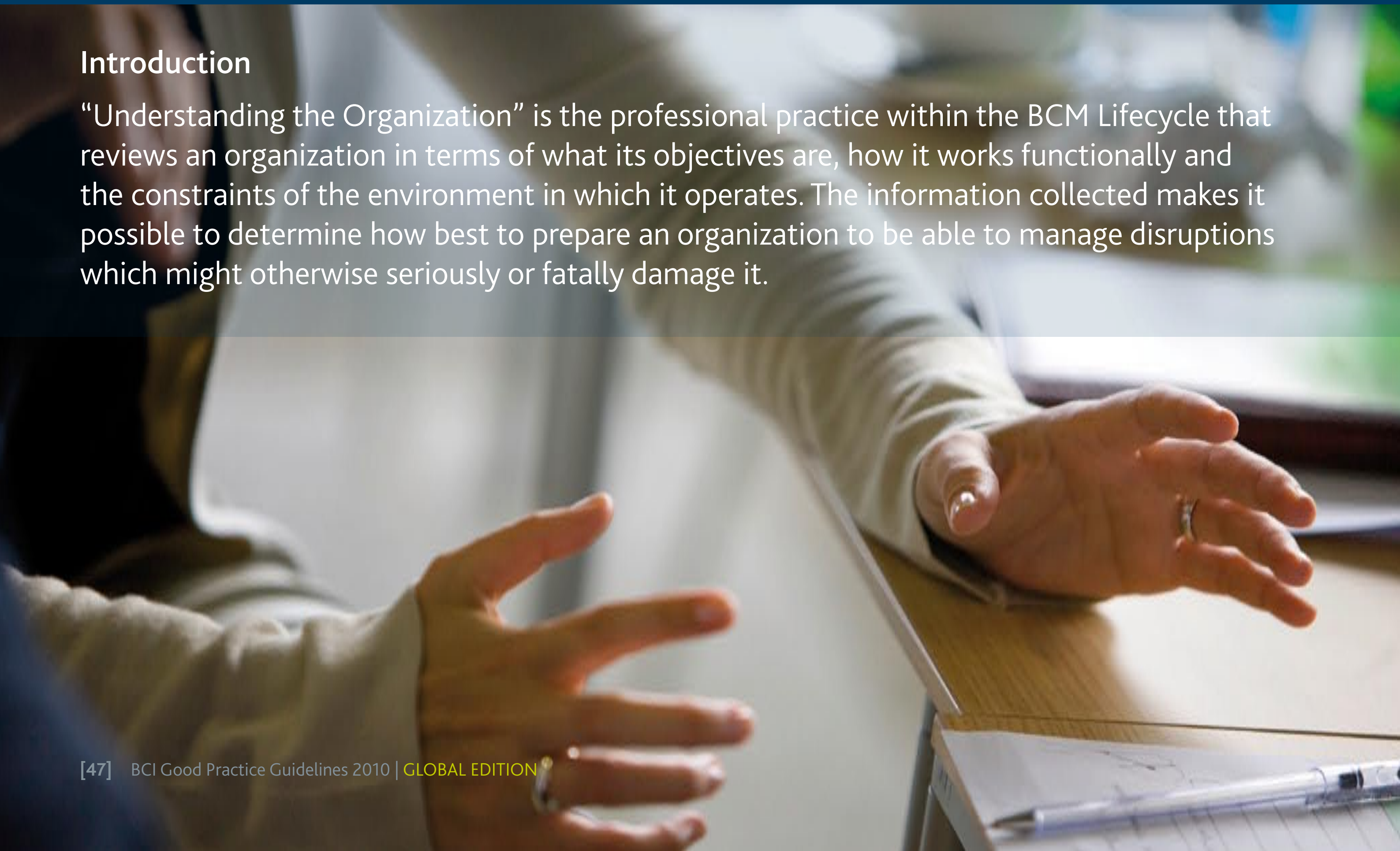
Certification of an organization against a formal standard does not guarantee that it will successfully manage all disruptions, only that the aspects of the process of BCM that can be objectively audited have been carried out.

However the rigorous nature of achieving certification does subject an organization to a considerable level of BCM exposure, and can build awareness of the subject among all levels of the organization. Certification, like regulatory compliance, is not the means to change culture in its own right but it does have an overall positive influence in that it requires an organization to be very clear about its BCM Policy and objectives and how it communicates them to staff.

# 03

# Understanding the Organization

# Understanding the Organization



## Introduction

“Understanding the Organization” is the professional practice within the BCM Lifecycle that reviews an organization in terms of what its objectives are, how it works functionally and the constraints of the environment in which it operates. The information collected makes it possible to determine how best to prepare an organization to be able to manage disruptions which might otherwise seriously or fatally damage it.

As described in the section on BCM Policy, the organization must make a prior, clear decision on whether the BCMS will cover the whole organization or just certain products or services. This sets the scope of the Business Impact Analysis (BIA), Continuity Requirements Analysis (CRA) and Evaluating Threats stages.

The tools for understanding your business for Business Continuity purposes are:

- **Business Impact Analysis (BIA)** – for evaluating the impact over time of a disruption to an organization's ability to operate
- **Continuity Requirements Analysis (CRA)** – to estimate the resources, facilities and external services that each activity will require at both resumption and return to normal after a disruption
- **Evaluating Threats through Risk Assessment** – to estimate the likelihood and impact on specific functions from known threats

The BIA identifies the urgency of each business activity undertaken by the organization; 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 CRA provides the information that will allow the scale (size and numbers) of the appropriate continuity measures to be determined.

Evaluating Threats through Risk Assessment helps in identifying potential causes of interruption to an organization, the probability of occurrence and the impact of the threat occurring. 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, this stage should focus on the inherent threats to the business activities identified as most urgent in the BIA results rather than on all threats to the organization.

The allocation of time and budget between the provision of recovery facilities and measures to mitigate specific threats must be decided by experience and judgement, as there are neither formulae nor rules to guide this decision.

A thorough BCM understanding of the organization through these techniques can often highlight business inefficiencies that would not otherwise be apparent to Top Management.

# Business Impact Analysis

## Introduction

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

A BIA can be used to identify the timescale and extent of the impact of a disruption at several levels in an organization. For example, to examine the effect of:

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

## Principles

It is necessary to obtain the full support of the Top Management 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, and 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 which can be used to decide the scope of the BCM programme.

Once the scope is determined, the BIA focuses on 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 organizations. However these activities may depend for their delivery on the support of other internal and external process, which must also be analyzed.

Examples of strategic activities include:

- Management
- Projects
- Planning

Examples of tactical activities include:

- IT (except for IT Service suppliers where this could be an external service)
- Human resources
- External support services such as utilities

Examples of operational activities include:

- Customer service
- Sales
- Production
- Home care visits
- Waste collection
- Provision of information to individuals or other organizations

Top Management should identify significant future plans for the organization which may affect the impacts to be evaluated in the BIA.

## Purpose

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

- To document the impacts over time that would result from its loss or disruption
- Identify the Maximum Tolerable Period of Disruption (MTPD) and thus the priorities for recovery – see *Concepts* below
- Identify the dependencies (both internal and external) 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
- 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 enable the organization to take advantage of the change to increase its resilience or improve its recovery capability.

## 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 irreparably damaged if delivery of a particular product or service cannot be resumed

  Factors that could be considered in estimating the MTPD include:

  > The impact on staff or public well-being
  > The impact of breaches of statutory duties or regulatory requirements
  > Damage to reputation
  > Damage to financial viability
  > Deterioration of product or service quality
  > Environmental damage
  > Other factors specific to the organization
- Seasonality and variability may affect the MTPD. As examples, a financial year-end may reduce the tolerable outage for the finance activity, while a one-off contract with significant time penalties may reduce the tolerable outage for a range of activities within the organization for the period of the contract

### Terminology

Care needs to be taken with the use of the word "critical". 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.

Having ascertained the MTPD for each activity it is often convenient to link activities with similar recovery requirements. Sometimes organizations call these groups according to the recovery timescale (e.g. one day, two day, one week etc.); others use the term 'critical' (or 'mission critical') for those activities required within the first few days. It would be better to use terms with less ambiguous, time related meanings such as 'time critical', 'time sensitive', 'priority' and 'urgent'.

### Assumptions

- It is assumed that the complex, inter-connected working of the organization can be understood by analysis of separate business activities
- Where resilience measures are already in place (such as alternative operating locations), these should be assumed to be in operation

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 that is, during the most disruptive period.

Whilst many activities are dependent on the continued operation of suppliers, it may not be possible to discover the service and recovery capabilities of these organizations.

### Sensitivity of Information

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

## Process

### Scope and Scale

- Identify the relationship between the various parts of the organization since this may affect the MTPD
- Where an organization has multiple sites, it may be necessary to decide on the maximum geographic extent of a disruption or extent of resource loss that the organization wants to, or needs to, plan to survive, in order to quantify impact. This should be documented in the BCM Policy and could be determined by:

  > Geographical extent (or market/customer area)
  > Regulatory or statutory requirements
  > Products, market sectors or specific customer requirements
- If the scale of the BIA will take too long, consider initially restricting its scope to a sub-set of products and services. The remainder can then be covered in a subsequent BIA
- Approval of the Terms of Reference for the BIA with the project sponsor.

### Business Impact Analysis

- Identify business activities across the organization (which may cut across several departments)
- Identify management owners for processes
- Identify suitable staff from whom information can be sought about the business processes – subject matter experts
- Identify how a disruption could result in damage to the organization's reputation, assets or financial position
- Quantify the timescale within which the interruption of each business activity becomes unacceptable to the organization because of its disruption to the delivery of products and services
- The collection of data for the Continuity Requirements Analysis (see later) may be undertaken at the same time

### Reporting

- Obtain approval by the process owner to confirm accuracy of information in the BIA
- Obtain support of the BCM sponsor for the conclusions of the BIA

## Methods and Techniques

### Data Collection

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 for 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. This is determined by the urgency with which each activity needs to be resumed
- The format of the data collection should be determined by how the results are to be presented
- The information required to establish the urgency of the performance of the activity being analyzed includes:
  > How long the activity takes to complete
  > Locations from which the activity is undertaken
  > Influences on the activity, e.g. peak periods, regulatory reporting
  > The impact of a disruption to this activity on activities within the organization
  > The time the organization can last without it
  > Any alternatives
  > The timescale within which the activity must be resumed

Factors to consider include:

- Volumes, e.g. calls per hour, output on production line
- Service level agreements, contracts, regulatory or legal requirements

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 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 deliver excellent results providing an appropriate level of detail and a standard reporting format that will assist in consistency of recording and analyzing information across multiple functions

### Software

There is 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 analyzing results, storage of information and reporting the results: their use does not remove the need for interviews with or involvement of individuals knowledgeable in the activity being analyzed.

### Reporting

Every organization has its own preferred style of reporting. The organization's 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 the information is collected, collated, analyzed and presented.

## Outcomes and Review

The outcomes from a Business Impact Analysis are:

- A list of Activities that contribute to the delivery of product and services within scope
- The Maximum Tolerable Period of Disruption (MTPD) and its justification for each activity. This will determine the time imperatives of the recovery strategies
- Activity dependencies – internal and external

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

- Major 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

The BIA process does not need to be repeated in its entirety at each revision – only those Activities affected by organizational change needs to be thoroughly reviewed. Other activities may require a sample review and confirmation of the previous BIA results.

# Continuity Requirements Analysis

## Introduction

The Continuity Requirements Analysis (CRA) collects information on the resources required to resume and continue the business activities to support the organization's objectives and obligations. This step is usually undertaken at the same time as the BIA information is being gathered.

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

## Concepts and Assumptions

### Continuity Requirements

It is often assumed that the resources required 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.

### Maximum Tolerable Data Loss (MTDL)

This is the loss of currency of data (electronic and other) from which an organization would be unable to recover its operational capability. The age of the data could make operations impossible, or the value of the lost data is substantial.

Some activities may be able to operate adequately with no data, or with data that is several weeks old. Other activities cannot tolerate any loss of data.

## Process

### Data Collection

This is to quantify the resources required over time to maintain the business functions at an acceptable level and within the maximum tolerable period of disruption. It should take into account any extra activity that will be generated by the interruption and the need to clear backlogs. The following resource categories may be considered:

- People – numbers, skills, etc.
- Premises – location, size, etc.
- Technology
- Information
- Equipment
- Supplies

### Reporting

- Obtain approval by the process owner to confirm accuracy of information
- Obtain support of the BCM sponsor for the conclusions
- Present to Top Management 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

There are a number of methods, tools and techniques to carry out a Continuity Requirements Analysis, including:

- Workshops
- Questionnaire (s) – paper and/or automated software
- Interviews (structured and unstructured), which are usually conducted at the same time as the BIA

## Outcomes and Review

The outcomes from a Business Impact Analysis are:

- An understanding of the resources required during the time after resumption to provide agreed service levels. This may be a simple number or a complex time-profile from initial to full resumption
- Acknowledgement of the Interdependencies – the activities that need to be operational (both internal and external) to maintain agreed service levels

This information feeds directly into the Business Continuity Strategy stage. The resource requirements will provide the data to evaluate alternative recovery solutions.

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

# Evaluating Threats Through Risk Assessment

## Introduction

The purpose of evaluating threats is to identify measures that can be put in place to reduce the likelihood of interruption to the organization's most urgent activities and the impact, should the risk be realised.

A BIA should be completed in advance, to identify the organization's most urgent activities.

The process of evaluating threats uses risk assessment techniques to identify unacceptable concentrations of risk to activities, and single points of failure, and identifies measures that can be put in place to lower the likelihood of disruption to them. The BIA documents the impacts over time that would result from a business interruption, and identifies both the urgency of product and service delivery and the activities which enable that delivery. This allows mitigation measures to be targeted at the most urgent activities within the organization thus improving the likely return on investment and minimal impact during disruption.

Many organizations have a well established Risk Management function, maintain a corporate risk register and have Risk Assessment embedded in the organization in as much as all managers are expected to assess risks as part of their normal practices and procedures. Threat assessments, therefore, may already be available for the organization's activities. However the presence of a Risk Management function is not a pre-requisite for an effective BCM programme.

In some countries and sectors the use of Risk Assessment is mandated. It will lead to a formal evaluation of risks and the consideration of appropriate measures to transfer, accept, reduce, or avoid the risks. However, evaluating threats as part of BCM is not the same as undertaking a Risk Assessment. Using risk assessment techniques as part of BCM may inform an existing Risk Management programme, but that is not its primary purpose.

## Risk Management Models

There are many Risk Management models in common usage, some of a general nature and others which have been entirely developed for a specific industry or sector. Virtually all of them involve identification of specific threats (or hazards) and use a formula to calculate a risk value based upon threat probability and threat impact (if threat is realised).

The simplest formula is:

- Risk Value = Threat Impact x Threat Probability

Other models use more complex formulae and include the level of mitigation already in place. Some risk models then order by assessing the ability to control that risk. This formula prioritises the threats that are easiest to control with the argument that this will give the best return on investment of time and money but do so at the penalty of ignoring many significant external impacts.

Whilst reasonably effective at dealing with Business as Usual (BAU) risks, many BC professionals believe that these types of risk assessment methods and techniques have serious shortcomings in evaluating catastrophic operational risks because:

- It is impossible to identify all threats
- Estimates of probability are guesswork or based on historic information
- The probability of an event occurring depends on the time period under consideration – the longer the time period the more likely it is that an event will occur
- The numeric scales often used to classify probability and impact (e.g. 1 for low, 2 for medium, 3 for high) over-emphasize the impact of minor events and cannot be used to calculate a comparative measure of risk (e.g. does a low probability and high impact risk have the same value as a high probability risk with low impact?)
- The use of a numerical scale to assign a value to impacts cannot adequately reflect the relative importance of less-quantifiable assets such as reputation
- The organization's 'risk appetite' or 'risk tolerance' is the amount of risk that an organization is prepared to accept and drives the level of action it will take to control identified threats

The above shortcomings demonstrate how difficult it is to measure risk and therefore to specify these metrics with any certainty.

## Process

The key steps in evaluating threats are:

- List the known internal and external threats that could cause disruption to the organization's most urgent activities, as determined in the BIA
- Determine a risk assessment scoring system for impacts and probabilities. Agree the approach with Top Management
- Estimate the impact on the organization of each threat using the agreed scoring system
- Determine the likelihood of each threat occurring and weight according to the scoring system
- Calculate a risk of each threat by combining the scores for impact and probability, according to an agreed formula
- Review the results of the scored risk analysis
- Prioritise the threats by level of risk
- Identify unacceptable areas of risk or single points of failure
- If the organization has an existing Risk Management control programme, pass the results of the threat evaluation to the person responsible for the programme
- Recommend the actions that can be taken to reduce the threat of disruption to the organization's most urgent activities

## Methods and Techniques

If the organization has an established Risk Management function, consider using the established risk assessment method or technique for evaluating threats.

Numerous risk assessment scoring systems can be obtained from published literature.

As well as the chosen risk assessment scoring system for impacts and probabilities, the methods and techniques that can be used to identify and evaluate threats include:

- The organization's risk register (if one exists)
- Determine internal and external threats from appropriate sources
- Event tree analysis
- Fault tree analysis
- Stakeholder analysis
- Scenario planning
- Threats identified during the BIA process
- Previous incidents experienced by the organization, the industry sector or the vicinity
- Known local natural or man-made hazards
- Geographical mapping
- Network analysis

Probabilities can be assessed using:

- Insurance statistics
- Published disaster frequency statistics

Specific threat reduction techniques and measures that can be adopted include:

- Taking advice on physical security – from the various national and international professional security associations, many of whom publish guidelines and good practice
- Taking advice on information security – from the various national and international Information Communication Technology and Information Security bodies. ISO 27001 and ISO 27002 will also provide valuable guidelines to follow
- Monitoring systems may provide prompt warning of utility failures, equipment failures and disruptive threats
- Sprinkler and fire suppression systems
- Resilient telecommunications networks so that there are no single points of failure

Proposed solutions can be evaluated using Cost Benefit Analysis.

## Outcomes and Review

The outcomes from evaluating threats are:

- A list of the threats that could cause a disruption to the organization's most urgent activities, prioritised by level of impact
- The identification of any unacceptable single points of failure
- Recommendations on actions to be taken to reduce the threat of disruption to the organization's most urgent activities

Threats to the organization's most urgent activities should be re-evaluated annually or more frequently if:

- The BIA has been updated
- 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

# Determining Business Continuity Strategy

# 04

# Determining Business Continuity Strategy

## Introduction

"Determining Business Continuity Strategy" is the professional practice within the BCM Lifecycle that determines which BCM strategies will meet the BCM Policy and organizational requirements and selects tactical responses from available options.

'Determining Business Continuity Strategy' uses the information obtained from the analyzes in the 'Understanding the Organization' stage of the BCM process to identify and select recovery and continuity options. This will enable the organization's activities to become operational following an interruption, before the organization's continued survival is threatened by their loss. It consists of three elements:

1 Identifying and Selecting Strategies
2 Identifying and Selecting Tactical Responses from Available Options
3 Consolidating Resource Levels

## General Principles

**Identifying and Selecting Strategies** identifies the strategies that are available to support the continued delivery of the organization's products and services within their already defined Maximum Tolerable Time of Disruption (MTPD) and Maximum Tolerable Data Loss (MTDL). It evaluates the advantages and disadvantages of each strategy, agrees the most appropriate strategies to further tactical investigation and finalises both Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each product and service.

**Identifying and Selecting Tactical Responses from Available Options** identifies the tactics that are available within the chosen strategies for each activity that the organization undertakes to deliver its products and services, identifies the costs and difficulties associated with each tactic, selects the most appropriate tactics for the activity, and the confirms that the resources provided will meet the recovery requirements and resume the activity with a RTO that is less than its MTPD and a RPO that is less than its MTDL.

**Consolidating Resource Levels** brings together all the resources that are to be provided through the selected strategies and tactics to deliver a consolidated view of the resource requirements. This is used to check that the strategies and tactics are viable when seen from an overall perspective, and to enable purchasing leverage when buying commercial business continuity services from third parties.

# Identifying and Selecting Strategies

## Introduction

The organization needs to select BCM strategies that will enable it to protect the continued delivery of its products and services. This section covers the identification and selection of these strategies.

A number of previously established parameters will be used as aids in the identification and selection of appropriate strategies. The MTPD is the duration after which an organization's viability will be irreparably damaged if a product or service delivery cannot be resumed.

The target time for resuming the delivery of a product or service following its disruption is known as its Recovery Time Objective (RTO).

The Maximum Tolerable Data Loss (MTDL) is the loss of currency of data (electronic and other) from which an organization would be unable to recover its operational capability. The age or value of the lost data could make resumed operations impossible. The target time for the worst case data loss in planning terms is known as its Recovery Point Objective (RPO).

An up to date BIA and CRA will provide the MTPD and MTDL for each product and service in the scope of the BCM programme. It will also quantify the recovery requirements for the activities that support the delivery of the products and services.

The RTO and RPO parameters for each product and service are determined in this section. This leads to the selection of the most appropriate BCM strategies.

## Concepts

Recovery strategies and the supporting tactical options need to be established which allow organizations to resume operations in a time-frame which meets both the RTO and RPO for individual products and services.

In order to do this effectively, certain concepts need to be considered in some depth.

### Balancing Cost and Speed of Recovery

In a very rare situation when cost is not a consideration, it would often be possible to define and implement a perfect solution. However in normal business practice, there is always a trade-off between cost and the speed of recovery, which needs to be balanced when selecting the most appropriate strategy. In most situations, it is true that the shorter the RTO the greater the cost to the organization, whilst the longer the RTO, the cheaper the solution. Of course a longer RTO also increases the chance that the recovery will not be achieved within the MTPD.

Consequently, the organization must always look to balance recovery capability against reasonable and affordable costs.

### Separation Distance and the Concept of "Off-Site"

In order to improve its continuity, an organization may keep duplicate copies of vital resources, use multiple suppliers, have replica operations in different locations, or have designated recovery sites. As many incidents frequently result in the loss of access to, or damage to a geographic area or location, there needs to be an adequate separation distance between the original and duplicate resources, the various suppliers, the replica operations, or the base site and its designated recovery site.

Since the incidents might result in complete destruction of a location, it is necessary to ensure that electronic and vital paper records are duplicated at another geographically separated location in a form that allows them to be:

- Readily accessible
- Recoverable for use within a defined timescale

Whilst greater geographical dispersion usually decreases the likelihood of two sites being affected by the same incident, there is no 'minimum' or 'correct' distance for separation. In fact for some threats, such as pandemics and global computer viruses, separation distance provides no protection against the likelihood of concurrent incidents being experienced.

For more conventional physical incidents, a few hundred metres is likely to provide only limited protection because of the way that emergency services use cordons and suspend or re-direct traffic flows. Some organizations can use their market or jurisdiction area to define the limit of their dispersion; others may choose the pragmatic alternative of placing a relocation site within the limit of how far they judge their staff could travel.

### Different Recovery Phases

There are three phases, or levels, to consider when identifying and selecting strategies to recover the delivery of a product or service after a disruption:

1 **Continuity** – to an initial minimum acceptable level
2 **Recovery** – to a sustainable level
3 **Resumption** – back to the normal level

A Continuity Strategy is required for each product or service, but Recovery and Resumption Strategies may not be necessary. Examples of such situations include where the:

- RTO is measured in weeks
- Minimum acceptable level is very close or equal to the sustainable level
- Organization may want to use the incident as an opportunity to change the way that it operates – in which case it may be appropriate to wait until after the incident before determining Recovery and Resumption Strategies

## Process

The following process needs to be undertaken for each product or service within the scope of the BCM programme:

- Identify the MTPD, and decide on the RTO, such that the RTO is less than the MTPD
- Identify the MTDL, and decide on the RPO, such that the RPO is less than the MTDL
- If there are any existing strategies, conduct a 'Gap Analysis' to identify where existing performance is measured against the required performance
- Identify suitable strategies that will enable the RTO to be achieved
- Analyze the strategies for effectiveness, and cost
- Provide Top Management with an evaluation of the strategies and a recommendation

Obtain agreement from Top Management on the strategies to be used. These should include the financial and resource provisions to determine and implement the tactical options that will be acceptable for each activity supporting the product or service.

## Scope

Strategies should include consideration of the following:

- Diverse Site
- Reputation
- Standby Facilities
- Subcontracting Work
- Post-incident Acquisition
- Insurance
- Do Nothing

### Diverse Sites

This requires the undertaking of activities for delivering the product or service at two or more geographically dispersed sites so that operations can be switched from one to another. Both sites are live. Whilst this strategy usually delivers a high degree of resilience, it can also be very costly and may not protect an organization if the incident has a worldwide reach, such as a pandemic or computer virus.This strategy is suitable where the RTO is measured in minutes or hours rather than days.

### Replication

A variation on diverse sites is to replicate the capability to undertake all the activities required at another geographically dispersed site, and to move the people to the replica site after the incident, one site is live while the other is dormant. This could be a facility obtained from a third party or provided by the organization itself.

This strategy may be suitable where the RTO is greater than a few hours and less than a day or so, providing the staff can be moved to the replica location quickly enough to resume the delivery of the product or service within the RTO. However, the strategy relies on staff being both able and willing to work away from their normal site for what could be a prolonged period of time.

### Standby Facilities

Where the RTO is greater than a day, an appropriate strategy may be to have a standby facility available than can be made operational within the RTO. Again, this could be a facility obtained from a third party or provided by the organization itself. This is particularly suitable where a facility has been temporarily shut down but capable of being made operational at short notice. It also relies on staff being both able and willing to work away from their normal site for what could be a prolonged period of time.

### Subcontracting Work

Some or all of the activities required to deliver a product or service can be subcontracted to a third party. For products and services that have a short RTO, these subcontract arrangements need to be established in advance, but for products and services that have a longer RTO it might be possible to wait until after the incident before entering into a contract.

Subcontracting can be particularly suitable for manufacturing, where the added cost of having diverse sites, replicas or standby facilities might be too expensive. However, in some situations, the only option for subcontracting may be to use another organization operating in the same market, which could be a competitor.

If the RTO is less than a day or so, and subcontract arrangements have been set up in advance, the strategy of keeping designs, templates and stocks of parts and raw materials at or close to the subcontractor's site can be an appropriate strategy.

### Post-incident Acquisition

For products and services that have their RTO measured in days or weeks, a suitable strategy may be to simply have a list of requirements and suppliers that can provide them at short notice. Order the facilities required after the incident has taken place.

This would not be an appropriate strategy for a product or service that requires specialist equipment, facilities or skills that are difficult to obtain.

### Insurance

Insurance, when properly arranged, can provide financial compensation for loss of assets, increased costs of working, business resumption and protection for associated legal liabilities. However it is unlikely to provide cover for the full expense of an incident including the loss of customers, impact of shareholder value or loss of reputation and brand image. It is important therefore, that the continuity options selected are consistent with the organization's insurance cover.

Business Interruption (BI) cover is most closely associated with BCM but it is important to note that typically this only covers business losses which are tied to another insurable loss (such as loss of premises). More recently some insurers have started providing cover for a wider range of interruptions such as supplier failure.

For SME (small to medium enterprises) businesses, insurance may provide some useful support following the loss of named key individuals due to death, injury or resignation.

### Do Nothing

In situations where the RTO is measured in months, waiting until after the incident to decide on a strategy to recover a product or service may be acceptable, particularly if the delivery of the product or service does not require any specialist equipment, facilities, or skills that are difficult to obtain.

## Outcomes and Review

The main deliverable is a set of BCM strategies that have been agreed by Top Management for each product and service in the scope of the BCM programme, plus an agreement to provide the resources to determine the tactical options to meet the strategic goals.

A review of the BCM strategies should be carried out after any recovery capability has been tested, and at least once a year following an update of the BIA and CRA. A significant change in any of the following should also prompt a review of the BCM strategies:

- Market conditions
- Acquisition or merger
- Products or services
- Regulatory or legislative requirements
- Customer demands

# Identifying and Selecting Tactical Responses

## Introduction

The purpose of this step is to select appropriate tactical continuity options for each activity that supports the delivery of the organization's products and services, and to identify what needs to be done to implement the selected options. These tactics will be based on the BCM strategies selected for each product or service.

Appropriate tactics for each activity will need to be selected to cover the requirements in the relevant areas of:

- People (skills and knowledge)
- Premises (buildings and facilities)
- Resources
  - > Information technology (IT)
  - > Telecommunications
  - > Non electronic (paper) information
  - > Equipment
- Suppliers (products and services supplied by third parties)
- For manufacturing organizations, particular attention will also need to be given to:
  - > Production processes
  - > Materials, logistics and inventory
  - > Power and utilities

In order to undertake this stage, both RTO and RPO parameters must be available with an up to date CRA that identifies the recovery requirement. The agreed BCM strategies for each product and service must also be available.

## Concepts

Determining recovery tactics and selecting appropriate solutions from available options is the most detailed part of the BCM Lifecycle. This is because it is:

a) the part of the process which will probably incur the most expenditure

b) the fundamental part of the technical and operational infrastructure that is needed to make plans workable in practice

In order to do this effectively, certain concepts need to be considered in some depth.

Consideration should be given to the following:

- Extent of planning
- Urgent activities
- Recovery time objectives for activities

- Options by time
- Reliability
- Re-appraising strategies
- Costs vs benefits
- Third party recovery sites
- The needs of diverse stakeholders
- The demands of civil emergency responders

### 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 resumption.

### Urgent Activities

Not all the activities associated with a product or service will necessarily need to become operational within the RTO set for the product or service, and in larger organizations, the sheer scale and difficulty of determining continuity options for every activity would be impractical. For these reasons, determining continuity options should concentrate on the most urgent activities. These will have been identified during the BIA, and will generally consist of those activities where the MTPD of the products and services that they support (and hence the RTO) is relatively short.

### Recovery Time Objectives for Activities

Where an activity must be operational to support the delivery of a product or service, the RTO for that activity must be less than or equal to the RTO of the product or service it supports.

### Options by Time

Continuity options for activities might change over time as the activity moves though the three levels of recovery:

1 **Initial Continuity** – to a minimum acceptable level

2 **Recovery** – to a sustainable level

3 **Resumption** – back to the normal level

### Reliability

When the options considered involve third party provision of services, there is often a management decision to be made between the cost and the reliability of third party provider. Promises may vary from verbal reciprocal agreements through 'best endeavours' to a contractually committed service level. The shorter the RTO, the more important the reliability of the delivery becomes.

### Re-appraising Strategies

It is not unusual to find that there is a need to re-appraise the BCM strategies for a product or service once the tactical continuity options have been reviewed for the activities that support its delivery.

### Costs vs. Benefits

It is difficult to use conventional cost-benefit analysis to justify the cost of protection or continuity measures because this requires assumptions to be made on the likelihood of incidents.

Manufacturing and service industries who supply other businesses may be able to demonstrate that increased sales or better margins can be achieved by demonstrating BCM capabilities (i.e. improved reliability) to their customers – and thus show a benefit compared to costs. This is more difficult to demonstrate when the service is non-commercial or is being provided as a public service.

### Third Party Recovery Sites

Third party alternative site arrangements are widely available in many countries. The options vary widely and are discussed in more detail in Annexe 1.

### The Needs of Diverse Stakeholders

There may be many individuals and groups affected by an incident. For example, in a major fire 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 organization's level of responsibility (both legal and moral) for these groups should be understood.

The organization should ensure that the needs of various stakeholders are satisfied when selecting continuity options, otherwise they may impede the subsequent recovery effort. For example, the local residents could press the local authorities to refuse permission to rebuild on a damaged site.

### The Demands of Civil Emergency Responders

The organization should be familiar with the procedures of the local emergency responders, and contact with these groups in advance may provide useful information to assist in selecting tactical options

Civil emergency responding organizations should implement their own BCM programme to ensure that disruption to their facilities does not hamper the response service that they provide to the community. In many countries, BCM planning is a statutory requirement for civil emergency responders.

## Process

The process includes the following steps:

- Identify the activities to be included for each product or service
- Determine the RTO and RPO for each activity in line with that for the product or service that the activity supports
- Identify tactical options for each activity

Analyze the options for effectiveness and cost

- Provide Top Management with an evaluation of the options and recommendations
  - > Obtain agreement from Top Management on the tactics to be used, including the financial and resource provisions for implementation
  - > Identify implementation projects for each of the tactics selected

## Scope

The scope of this part of the process is complex and demanding. Often technical advice might need to be sought from experts in other fields, in particular for manufacturing businesses. Typically specialists in purchasing and supply, inventory management and capacity planning might be needed to help determine tactics that would be appropriate.

In general terms, the BCM professional needs to ensure that the following areas are addressed properly in any tactical solution:

- People
- Premises
- Resources
- Suppliers

Due to the vast differences in types of businesses that will implement BCM, it is not possible in such a Guide as this to be prescriptive about what tactics will be suitable for which companies, sectors or geographies. However Annexe 1 provides considerable advice which should help with the selection and decision process.

Although the options selected need to work in isolation (e.g. in the event that the only loss is of a computer system or single production line), they also need to work together (e.g. when a building is lost in a disaster that destroys all the resources in the building, renders some of the staff unavailable for work, and also disrupts a local time critical supplier).

## Outcomes and Review

The outcomes and deliverables from this stage are:

- An agreed set of tactical continuity options agreed by Top Management
- Funding and resource approval to implement the agreed tactical options
- A list of projects for implementing the agreed tactical options

Another outcome may be to re-appraise the BCM strategies selected for a product or service if tactical options prove unavailable or costly.

A review to ensure that the appropriate continuity options have been selected for each important and urgent activity should be carried out at least every 12 months, and following any change to the BCM strategies for any of the products and services that the activity supports.

Any significant change in the following may also trigger a review:

- The skills required to undertake the activity
- The premises at which the activity is undertaken
- The resources used by the activity (particularly IT)
- The suppliers on which the activity is dependent

# Consolidating Resource Levels

## Introduction

The purpose of consolidating resource levels is to:

- Ensure that the selected tactics are consistent across the organization
- Ensure that the selected tactics do not conflict with one another (e.g. that different activities are not planning to use the same internal resource for recovery)
- Determine how best to source external requirements (e.g. third party recovery sites)
- Assist in determining the number and structure of the Business Continuity Plans

Having selected appropriate tactical continuity options for each important and urgent activity, the resource requirements of the tactics need to be consolidated.

## Concepts and Assumptions

It is often assumed that the required services will be commercially available. In many countries this is not necessarily the case, and some governments will not permit organizations to source such services outside their country boundaries.

When the third party recovery services required by the consolidated tactics are not available, this will lead to the organization re-evaluating both the BCM strategies and the tactical continuity options. One outcome of this may be that the organization decides to provide its own recovery facilities, and then offer to share them commercially with other organizations faced by the same dilemma. This approach is particularly relevant in countries in which third party providers have yet to establish a business presence.

## Process

This process is made up of the following steps:

- Aggregate the recovery requirements from the selected tactical continuity options
- Check that the selected tactics are consistent across the organization
- Check that the selected tactics do not conflict with one another
- Check that the consolidated third party recovery requirements can be obtained
- Re-evaluate the tactical continuity options, if found to be inconsistent or in conflict
- Provide Top Management with an evaluation of the consolidated requirements
- Obtain agreement from Top Management for any changes to the tactics to be used, including the financial and resource provisions for implementation
- Update the projects identified for implementing the agreed tactical options, as required
- Establish the projects for implementing the agreed tactical options

## Outcomes and Review

The outcomes and deliverables from the Consolidating Resource Levels include:

- A set of projects for implementing the agreed tactical options
- A consolidated set of third party resource requirements to be used in purchasing the resources
- Details of the tactics and recovery resource requirements that will be used in developing the Business Continuity Plans

Consolidating Resource Levels should be reviewed whenever there has been a change in the selected tactical continuity options for an activity.

It should also be reviewed when there has been a change in the organization that might affect the provision of in-house recovery resources, and when a recovery contract with a third party comes up for renewal. This might result in a change to either the recovery strategy or the tactical means of delivering it.

> "When the third party recovery services required by the consolidated tactics are not available, this will lead to the organization re-evaluating both the BCM strategies and the tactical continuity options"

# Developing and Implementing a BCM Response

# 05

# Developing and Implementing a BCM Response

## Introduction

"Developing and Implementing a BCM Response" is the professional practice within the BCM Lifecycle that implements agreed strategies through the process of developing a set of Business Continuity Plans.

The aim of the various plan (s) covered in this stage is to identify, as far as possible, the actions and the resources which are needed to enable the organization to manage an interruption whatever its cause, back to a position where normal business processes can resume.

The key requirements for an effective response are:

- A clear procedure for the 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 structures, and whatever structure is adopted, it is important that the chosen strategy fits with the culture of the organization.

The actions outlined in plans are not intended to cover every eventually as, by their nature, all incidents are different. Procedures may need to be adapted to the specific event that has occurred and the opportunities it may have opened up.

## General Principles

Although the term 'Business Continuity Plan' (BCP) implies a single document, in reality this covers a number of different activities and will usually consist of multiple plans. The BCP can exist at any organizational level and can go down to any level of procedural detail. It can cover a complete organization or part of an organization, and can be scoped by products, services, locations, divisions, departments and in specialist circumstances, for particular scenarios. However, there are five types of plan corresponding to five overlapping stages of the response, and any of these can appear in any BCP at any level. The five stages are:

1. **Emergency Response** – the immediate response to an emergency, such as an Evacuation Plan
2. **Incident Management** – the management of the response to the incident, such as a Crisis Communications Plan
3. **Continuity** – the initial business response to ensure that essential activities can continue to operate at a minimum acceptable level
4. **Recovery** – a plan to recover activities to a sustainable level
5. **Resumption** – a plan to resume operations at what the organization defines as "normal"

The nature of most business activities can be classified as strategic, tactical or operational, and Business Continuity practitioners must recognize that all three elements are usually present to some degree in all BCPs. It is important that BCPs address all three levels and their related issues. However, there is no absolute definition of what is strategic, what is tactical, and what is operational. How they are viewed is often determined by context rather than by theory. This means that there is no single solution for how to structure plans. It also shows that both general business experience and BCM knowledge need to be combined to find the optimal structure for an individual organization.

## Types of Plans

The term Business Continuity Plan (BCP) can be defined as:

> A documented collection of procedures and information that have been developed, compiled and maintained in readiness for use in an incident, to enable an organization to continue to deliver its important and urgent activities, at an acceptable pre-defined level.

There are other terms in common usage, all of which are specialist forms of the BCP. Although clearly within the generic definition above, Emergency Response Plans and Incident Management Plans are managed separately from BCP in some organizations. In some organizations, ICT (Information and Communication Technology) departments still refer to their plans as Disaster Recovery Plans.

Other names for specialist plans include:

- Crisis Management Plan
- Media Response Plan
- Product Recall Plan
- Pandemic Plan
- Continuity of Operations Plan

In the context of this guide, all plans (however named) which conform to the generic definition are considered BCPs.

# Incident Response Structure

## Introduction

Regardless of the cause the incident which causes a business interruption or impact, there must be a documented and fully understood incident response structure in place. This structure will cover three types or levels of management activities.

1 Strategic
2 Tactical
3 Operational

The response structure adopted by an organization needs to address all these levels, and for each plan that is developed and implemented as part of the structure, a response team with clear procedures for escalation and control needs to be established.

An example of this is the technique used by the UK Emergency Services, who define these three levels of incident response as Gold, Silver and Bronze. When applied to an organization's response structure the responsibilities of this model are shown: (see below).

This model is only one example of a suitable response structure, although the need to escalate information upwards and communicate decisions downwards is an essential feature in any response model. The approach is particularly effective in the two initial phases associated with BCP implementation – Emergency Response and Incident Management.

## Incident Management Plan (IMP)

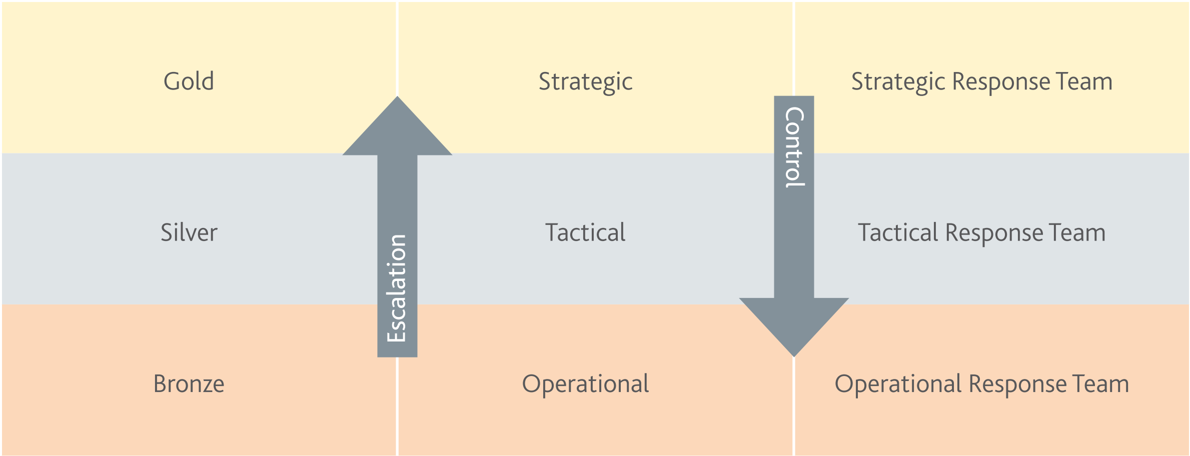
Although this is part of the Business Continuity Planning process, it is often considered as a unique BCP in its own right. It has some special characteristics which differentiate it from the tactical and operational plans which form the bulk of the BCP portfolio. It is defined as:

> A documented plan of action for use at the time of an incident, covering key personnel, resources, services and actions needed to implement the incident management process.

This is a strategic level BCP that defines how strategic issues resulting from a major incident would be addressed and managed by Top Management. The plan may also be used when the incident is not entirely within the scope of the BCM programme. This might include crises that do not result from interruptions, such as a hostile take-over or negative media exposure, and those where the impact is over a wider area than allowed for in the BCM strategy, such as a national emergency.

The media response to any incident is usually managed at the strategic level, though some organizations could manage it at a tactical level.

The IMP is sometimes called a 'Crisis Management Plan'; however reporting in the media that an organization has invoked its 'Crisis Management Team' may lead people to think the organization feels that it has a Crisis. The term 'Incident' has less negative connotations so is preferred in this document.



| | | |
|---|---|---|
| Gold | Strategic | Strategic Response Team |
| Silver | Tactical | Tactical Response Team |
| Bronze | Operational | Operational Response Team |

## Tactical Level Plans

Tactical level plans often form the bulk of an organization's portfolio of BCPs. These plans address business disruption, interruption or loss from the initial response to the point at which business operations are recovered, and are based upon the agreed Business Continuity Strategies. A tactical level plan coordinates the recovery, ensuring that the operations covered by the plan work together to a common purpose, and that, where resources are scarce, they are allocated to the most urgent activities.

Where there are multiple operational level plans, one of the roles of the tactical response team is to sort out any conflicts between these plans to ensure that the recovery is coordinated. The tactical level plans may change the agreed priorities and recovery strategies to take into account seasonal changes, and business conditions, or on direction by Top Management.

If the event falls outside the scope of the assumptions on which a tactical level plan was based, then the situation should be escalated to Top Management, who manage the strategic level issues.

## Operational Level Plans

Operational level plans provide for the resumption of the business functions covered by the plan from the beginning of the incident through the recovery phase back to 'business as usual. They are based upon the agreed recovery requirements and Business Continuity tactics, and provide procedures and processes for recovering activities to the agreed levels of operation.

For departments managing infrastructure, operational level plans will provide a structure for restoring existing services or providing alternative facilities to support the recovery of other business units. Plans may also be written for other support services, such as Human Resources (HR), that may have a specialist role in supporting the recovery or provide specialist advice.

## Timeline

The response teams at the three levels may not necessarily invoke their plans simultaneously. Invocation may start at the operational level and escalate to the strategic level. Alternatively, invocation may start at the strategic level and cascade down to the operational teams. As the organization starts to recover and resume its normal operations, it is likely that the strategic team will stand down first, followed by the tactical teams, and lastly the operational teams.

## Process

These levels of response provide a suitable model for all sizes of organization, but need to be implemented in a way that fits the organization's management structure and culture. Examples of how the levels might be implemented in different types of organization are provided below.

### Small, Single Site Organization

In a small, single site organization, all the levels of response might be implemented as a single plan with a single response team covering all aspects of the strategic, tactical, and operational response.

### Medium Sized Organization

In a medium sized organization, the levels of response might be implemented as:

- **Strategic** – an IMP, with a response team made up of the Top Management
- **Tactical** – a single BCP covering the recovery of all the organization's operations, with a response team consisting of the operational management
- **Operational** – covered by the BCP (except for ICT, which because of the technical detail required, has its own operational recovery plan with a technical ICT response team)

### Large Organization

In a large organization, the levels of response might be implemented as:

- **Strategic** – an IMP, with a response team made up of the Top Management
- **Tactical** – a number of BCPs, each one covering a major division, product, service or location, each with its own response team consisting of the operational management responsible for the areas covered by the BCP
- **Operational** – covered by the individual BCPs, (except for the main support functions of ICT, Finance, Facilities, and HR, each of which has its own specialist response team)

### Large Multi-National Organization

In a large multi-national organization, the levels of response might be implemented as:

- **Strategic** – a global IMP, with a response team made up of the Top Management with global responsibilities, and an IMP for each territory, with a response team consisting of the Top Management from the territory
- **Tactical** – each territory to have a number of BCPs, each covering a major division, product or service, each with its own response team consisting of the operational management responsible for the areas covered by the BCP
- **Operational** – each department or location covered by a BCP to have its own detailed operational recovery plan, with its own response team made up of the operational managers of the department or location, and separate plans for the main support functions of ICT, Finance, Facilities, and HR, each of which has its own specialist response team

> "Operational level plans provide for the resumption of the business functions covered by the plan from the beginning of the incident through the recovery phase back to 'business as usual"

## Developing and Managing Plans

### Introduction

The incident response structure selected, the BCM strategy, and the size and diversity of the business will determine the number and type of plans to be put in place.

Ideally, tactical and operational plans will not be developed until the organization's Strategy has been determined and agreed, although for organizations with no arrangements in place, the strategic level response (typically an IMP) may be implemented beforehand to provide limited protection in the meantime.

Each plan should always contain assumptions about the maximum scale of the incident in terms of extent, duration or staff impact.

### Process

The key steps in developing a plan include:

- Appoint an owner
- Define the objectives and scope
- Develop and approve a plan development process and programme
- Create a planning team
- Create a response team
- Agree the responsibilities of the response team and their relationship with other plans and response teams (strategic, tactical and operational)
- 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
- Draft the plan
- Circulate the draft plan for consultation and review
- Gather feedback from the consultation
- Amend the plan as appropriate
- Agree and validate the plan, for example by using it in an exercise
- Agree a programme of ongoing exercising and maintenance of the plan to ensure it remains current

## Methods and Techniques

The methods, tools and techniques to enable the development of plans include:

- Scenario planning
- Interviews (structured and unstructured)
- Checklist(s)
- Workshops
- Identified threats
- Previous incidents
- Known local hazards

## Format and Content

Plans should be concise and easy to read. They can be modular in design so that separate sections can be supplied only to those teams that require them. If this approach is adopted it is important that someone retains an overview co-ordination role.

A number of methods and techniques can be adopted to develop the plans and these are described later in this chapter. Whatever method is used, however, plans should not be developed in isolation and everyone that has an identified role should be consulted during the development stage.

### Contents

All plans, whether they operate at the strategic, tactical or operational level should contain a number of similar elements:

- Purpose
- Scope
- Objectives
- Assumptions
- Incident management structure (for the organization as a whole)
- Response team responsibilities
- Response team membership
- Individual responsibilities of the response team members
- Invocation instructions
- Authority to invoke
- Team mobilisation instructions
- Team meeting room (command centre) locations
- Communications (covering staff, stakeholders, customers, media, etc.)
- Action lists
- Key information from previous stages of the BCM Lifecycle
- Contact details (usually held as appendices)

The plan should contain initial prompts for action, and any specific actions or decisions the team may need to make.

## Roles and Responsibilities

The roles of the team and specific individuals should be documented, and deputies should be identified for each role.

Responsibilities for the team or nominated individuals may include:

- Team leader – who should ensure that the response team is properly staffed and be able to make appointments if necessary
- Internal communications – to agree the resumption timetable with other response teams
- External communications – stakeholders and the media
- Operations
- Technical support
- Administrative support
- Logger – to maintain 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 flexibility and encourage action where there is doubt since it is easier to stand a team down rather than activate them after the incident has developed.

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, depending on the nature of the incident, may meet continuously, at set periods throughout the day, or daily.

### Meeting Room

For large-scale disasters or very geographically spread organizations the concept of a virtual Incident Management Team with a virtual command centre might be suitable, provided the telecommunication capabilities and shared access to time critical information can be guaranteed.

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

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

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

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
- Stationery
- A means of logging all actions
- Refreshments
- Nearby or on-site sleeping facilities

Hardware and information can be kept off-site at the alternative location in a locked trunk often called a 'battle-box', 'grab bag', or 'recovery box'.

## People Activities

Organizations have a responsibility (which may be legally enforced) to safeguard the welfare of their employees, contractors, visitors and customers. 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:

- Special needs including:
  - > Pregnancy
  - > Disability
  - > Family responsibilities
- Dealing with issues relating to serious injuries or fatalities (in consultation with the emergency services and in accordance with local regulations and customs)

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
- 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 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 organization's own staff.

Once emergency services have departed, the organization will resume responsibility for its own site security.

### Communication

Communication may need to be carried out with the following:

- Staff, relatives, friends and emergency contacts
- Customers
- Suppliers
- Members or sections of the public
- Shareholders, investors, board members or owners
- Other parts of the organization
- Regulatory authorities
- Media – local and national newspapers, radio, TV, internet and other media

Response team responsibilities for communicating with each of these groups should be agreed upon as part of the development of the incident response structure.

## Media

The strategic level plan should address how the organization will manage communication with the media, but all plans should include reference to the media plan and instructions to staff on what they should do if approached by the media. They should also contain information on what actions staff should take if they are involved in an incident which is likely to attract media attention and who should they inform.

## Quality Assurance

Methods and techniques that can be used to assure the quality of plans include:

- Checking that the plans reflect the information collected and documented from the previous stages of the BCM process
- Checking that the plans reflect the agreed BCM strategies
- Checking that the style of the plans reflect the organization's culture
- Reviewing the best way to hold contact telephone numbers, and whether or not they should be included in the plans
- Reviewing the use of names of individuals and/or job titles in the plans (the use of names can lead to frequent changes to a plan)
- Considering how a plan can be made smaller if it is too large
- Checking that the plans conform with the agreed BCM document control standards
- Checking that the sections of the plans are in a logical sequence
- Getting someone who doesn't know the plans to read through them and point out any further detail or information they would need to implement the plans
- Checking that the plans are readable – although the format and layout of the plans is likely to vary from business to business, there are a number of tips that can be adopted to make the plans easier to use (such as using section dividers, coloured paper and appendices)
- Making sure that the plans do not contain unnecessary information

## Outcomes and Review

The outcome of the process is a set of up to date and effective plans covering the strategic, tactical, and operational response to incidents that might cause serious disruption to the organization's operations.

The BCM programme should identify a maintenance regime and any changes that result from this need to be fed back into the planning process to ensure plans and procedures are kept up to date.

# Strategic Plans

## Introduction

Although the basic principles and approach to producing BCPs is similar in all situations, different degrees of emphasis are needed for different levels of plan. The need to involve Top Management in the development and implementation of BCPs is essential both to immediate successful response and to ongoing Business Continuity. Case studies of major incidents suggest that effective and rapid management of a crisis is the significant factor in protecting an organization's brand from financial and reputation damage.

Some incidents will require a strategic level response that does not result from disruption to activities (for example those involving threats to reputation alone), and may therefore not involve a full BCP response. However, where a full BCP response is required there is almost always a need to involve the strategic level team if only to make them aware of the situation in case it escalates.

For organizations with no plans in place, a strategic level plan may be the first element to develop, thus providing a limited amount of protection while other plans are produced. The terms used in these Guidelines for the various plans are not universally applied, so it is important that an organization chooses names that fit into its own culture and structure, and that the roles described here are included.

## Methods and Techniques

Templates can be used to assist with the implementation of standard procedures.

## Contents

As, by their nature, all crises are different, a strategic level plan is a set of components and resources that may be useful to the team tasked with activating the plan, and should include a communications element. The content will also depend on the nature and complexity of the organization, but should include most of elements listed.

The strategic plan may contain reference material on the strategies of different parts of the organization or generic information on how a loss of building or major loss of IT is to be recovered. This is not to micromanage the incident, but to inform the team of how the recovery will take place, and the timescales that may be involved.

## Responsibilities

The strategic response team members are the guardians of the organization's reputation and have responsibility to adjust the organization's recovery strategy if its reputation is being threatened. Specific responsibilities of the strategic response team include:

- Determining the recovery policy
- Establishing the strategic objectives of the response to the incident
- Devising a long term strategy
- Managing communications, in particular with the media (see below)
- Approving significant expenditure
- Monitoring the overall progress of recovery
- Identifying and maximizing opportunities or advantages arising from the incident
- Ensuring that the recovery is in line with the long term interests of the organization
- Approving media statements before they are issued to devising, monitoring and adjusting as necessary the media strategy
- Ensuring financial health of the organization
- Ensuring that any recovery meets the organization's legal obligations

## Resources

Specific resources that could be considered for use by the strategic team in addition to those identified earlier for all plans include:

- TV/radio 'studio' facilities – to rehearse interviews
- Communications line and camera for transmitting interviews straight to broadcast station and video-conferencing
- A separate and nearby venue for hosting the press

## Media Plan

The media plan should address how the organization will manage communication with the media. The plan may be included within the strategic or tactical level plan, or it may exist as a separate document.

The media plan should include:

- Deciding in advance who the spokesperson(s) will be ensuring:
  > The person has been trained in their role
  > There are sufficient people to brief the media at a central location as well as to be on site at a local incident
  > There is a designated technical spokesperson if appropriate

If appropriate, work with specialists such as public relations companies to develop the organizations media response, and consider retaining a company for use during an incident. If possible, develop a relationship with key media people in advance of any incident.

- Identifying the audiences
  > The possible audiences should be segmented and then a plan should be made of the most appropriate method for putting across the message to each e.g. local radio, national newspapers

The response to each method should be monitored and reviewed. This could include use of a media monitoring/cuttings service.

- Consider the likely messages
  > Develop questions and answers for the most likely incidents
  > Develop a set text on the organization which can go out to describe the company in media statements
  > Develop contact lists for media organizations
- Develop a process for media statements, how they will be approved and communicated to the media
- Document how the media statement will be communicated throughout the organization

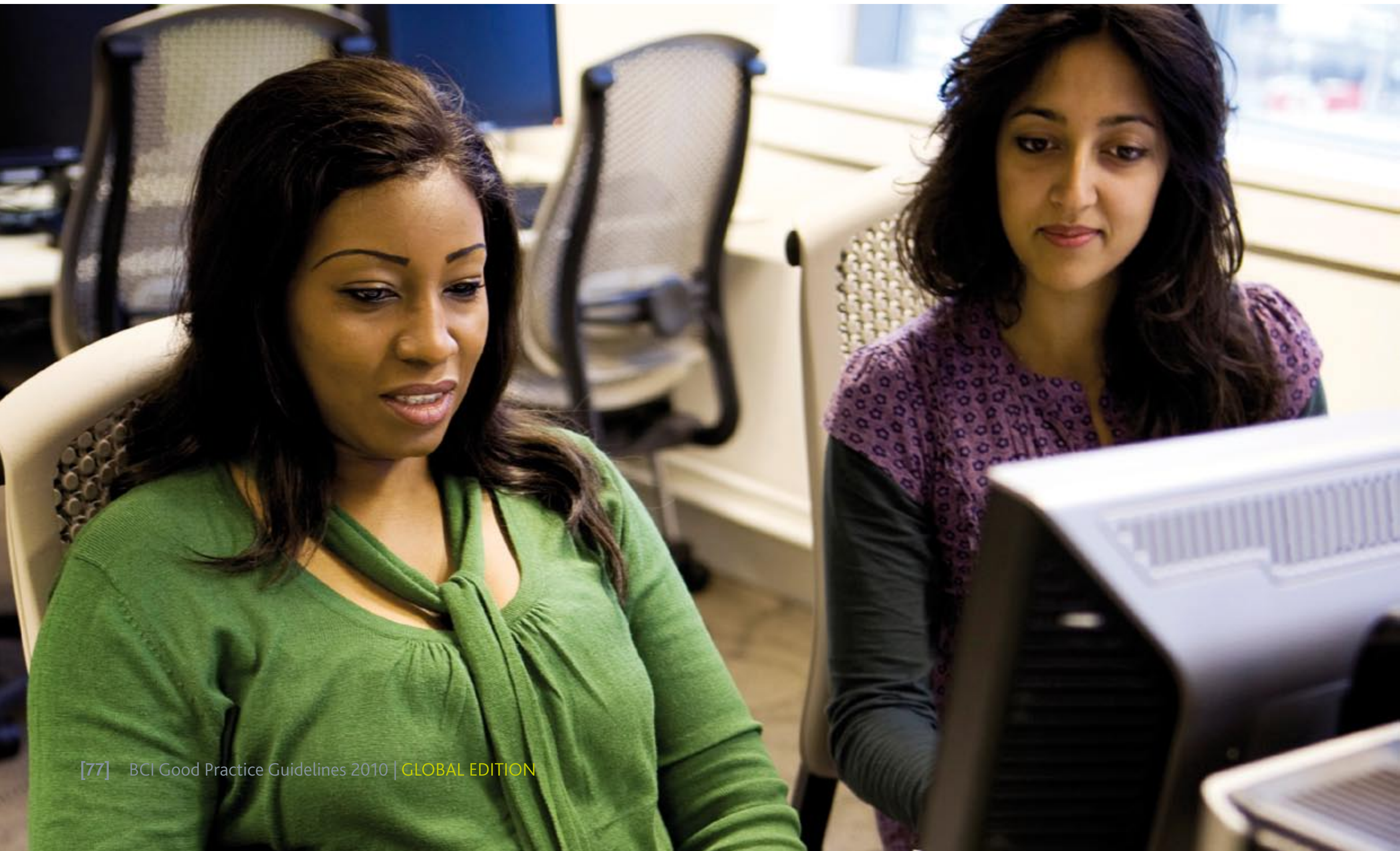
## Outcomes and Review

The outcomes of the strategic planning process include:

- A plan that can support the role of the organization's Top Management during a crisis
- A plan for managing media and stakeholder communications 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

A 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 Top Management change, or by significant change in the external operating environment.



# Tactical Plans

## Introduction

Tactical level plans are the most common form of BCP. They pull together the response of the whole organization to a disruptive incident by facilitating the resumption of business activities. Those using the plans should be able to analyze information from the response teams concerning the impact of the incident, select and deploy appropriate strategies from those available in the plans, direct the resumption of business units according to agreed priorities and pass progress information to the strategic level response team.

The content of a tactical level plan will vary from organization to organization and will have a different level of detail based on the culture of the organization and the technical complexity of the solutions. It is rarely possible to write an effective tactical level plan unless the key elements of the resumption strategy are in place or are well advanced in their planning.

## Methods and Techniques

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

A tactical level plan will always contain assumptions relating to the scale of the incident covered (in terms of extent, duration or staff impact). If the scale of the incident exceeds the assumptions, then this should be escalated to the strategic level response team.

Specific steps in developing tactical level plans may include:

- Appoint a person to manage the development of all the tactical plans
- Develop a planning process and timetabled programme. Where possible, begin with the plans for the most urgent business activities
- Decide the structure, format, components and content of the plans
- Develop an outline or template plan to encourage standardization of documentation but allow individual variations where this is appropriate

A variety of software products is available to assist in building and maintaining a tactical level plan, but these are 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.

## Contents

Tactical level plans should contain sufficient information to enable the tactical level response teams to continue or recover the business activities covered by the plan.

It should include detailed procedures for the team to:

- Respond to invocation
- Make decisions
- Mobilise resources
- Initiate activity recovery
- Receive information from other teams
- Report status to the strategic level team

For other items that might be usefully included, see '*Format and Content*' on page 72.

## Responsibilities

Specific responsibilities of tactical level response teams may include:

- Coordinating and monitoring the operational level of recovery
- Allocating available resources to operational teams
- Changing the agreed priorities and recovery strategies to take into account seasonal changes, business conditions or on direction from the strategic level
- Coordinating main support functions of ICT, Finance, Facilities, and HR
- Receiving or seeking information from other response teams
- Reporting to the strategic response team
- Mobilising third-party suppliers of salvage and recovery services

### Resource Requirements

Available resources might include lists of:

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

Vital information might include:

- Customer information
- Contact details
- Legal documents – such as contracts and insurance policies
- Service level agreements

### Outcomes and Review

The review of the tactical planning process includes:

- Tactical level plans which should be approved by Top Management
- A framework within which the operational level plans can work

Some information within tactical level plans such as contact details should be reviewed in line with BCM 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
- A major business process change
- A significant change in staff
- A change in the supplier of BCM solutions

## Operational Plans

### Introduction

Tactical level plans will rapidly become unwieldy if all recovery procedures are included in a single document. When this becomes the case, the response and recovery plans of each business unit should be made into one or more separate operational plans that become the responsibility of the business unit to which they relate.

Operational level plans cover the response by each department or business unit to the incident. Examples of operational plans are:

- A business department plan to resume its functions within a predefined timescale
- Procedures to assist an incident response team, usually lead by a Facilities department that deals with the specific incident and its physical impact
- A Human Resources response to welfare issues during an incident
- 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 plan covers a single activity or a department covering several activities.

Likewise the operational plans may be supported by more detailed plans for specific responses, locations or equipment.

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

### Methods and Techniques

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

Specific steps of the operational plan development and planning process include:

- Appoint a person to manage the development of all the operational plans

> "Operational level plans cover the response by each department or business unit to the incident"

- Appoint a representative within each business unit to develop their plan
- Develop a planning process and timetabled programme. Where possible, begin with the plans for the most urgent business activities
- Decide the structure, format, components and content of the plans
- Develop an outline or template plan to encourage standardization of documentation but allow individual variations where this is appropriate
- Ensure that business units nominate individuals to fulfil roles within their plans
- Manage 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 business unit
- Gather feedback from consultation
- Amend plan as appropriate
- Validate the plan through a unit test
- Document connections with the tactical level plans and between operational plans
- Conduct a resource requirements analysis across all plans to define resource requirements for support functions

## Contents

Specific operational plans may include instructions regarding:

- Facilities
- Staff welfare
- Business unit resumption
- IT disaster recovery

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

- Building evacuation and safe shelter plans
- Bomb threat plans
- Evacuation points (including alternate or off-site)
- Emergency services liaison
- Redeployment of staff and visitors
- Salvage resources and contracted assistance
- Escalation circumstances
- Human resource and welfare issues
- Health and safety liabilities
- Procedures for accounting for staff
- Procedures for contacting staff
- Counselling and rehabilitation resources
- Escalation criteria
- Escalation procedure to tactical level teams
- Response to initial contact from tactical level teams
- Contacting team members
- Resumption plan for each activity
  > Staff numbers
  > Key contacts
  > Procedure for resumption of business activity
  > Activity priorities
  > Special procedures
  > Work in progress issues
  > Consumables required

## Outcomes and Review

The outcomes of the operational planning process includes:

- Documented operational plans for business units
- Criteria and procedures for each business unit to escalate issues
- Clearly defined BCM roles within the business units

Operational plans should be reviewed if there is a major change in the business process or technology within the business unit and when changes are made to the tactical level plans.

# 06 Exercising, Maintaining and Reviewing BCM

# Exercising, Maintaining and Reviewing BCM

## Introduction

“Exercising, Maintaining and Reviewing BCM” is the professional practice within the BCM Lifecycle that seeks to ensure continuous improvement is achieved through the ongoing and scheduled actions. The activities undertaken in this section will be underpinned by the BCM Policy discussed in professional practice Number 1.

### General Principles

Most organizations exist in a dynamic environment and are subject to changes 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 organization it supports, it must be current, accurate, complete, exercised and understood by all stakeholders and participants.

# Developing an Exercise Programme

## Introduction

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 relevant personnel (including deputies) are exercised

Business Continuity Management (BCM) capability cannot be considered reliable until it has been exercised. An Exercise Programme should focus on maximizing business benefits while minimizing business disruption. A planned Exercise Programme is required to ensure that all aspects of the plans and personnel have been exercised over a period of time, avoiding disruption to the whole business.

Exercising can take various forms, including technical tests, desktop walkthroughs and full live rehearsals. No matter how well designed a BCM Strategy or Business Continuity Plan (BCP) is, a series of robust and realistic exercises will identify issues and assumptions that require attention.

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

Validating technical recovery capabilities is an important part of an exercise programme but an equally key element is the role of people. The programme should ensure that their skill levels, knowledge of their role, management capability and decision-making are exercised in a safe environment.

While a service may be outsourced, the accountability for Business Continuity cannot. The organization outsourcing the service must ensure that the suppliers can cope with disruption. Ideally, BCM will form a part of the outsourced contract and will include a shared exercise programme relevant to the recovery objectives of the customer.

The BCM Policy should outline the responsibilities for the Exercise Programme.

## Process

- Discuss with Top Management any perceived areas of weakness that would benefit from the visibility an exercise provides
- List all recovery processes linked with the activities that will be tested (e.g. resource allocation, contact sheet, relocation)
- Decide on suitable type of exercise activity for each process
- If exercises have been conducted in the past, review the supporting documentation to avoid a replication of scenario or people, and to identify the activity that requires further exercising
- List all personnel or groups involved in each process
- Devise a timetable of exercise activities that ensures that, over a period, all relevant personnel take part in the exercise

The exercise programme should include suitable activities to exercise the various elements 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 manner?
- **Timeliness** – can the procedures achieve the required Recovery Time Objective (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?

> "An exercise programme should focus on maximizing business benefits while minimizing business disruption"

## Methods and Techniques

To be successful an Exercise Programme must begin simply and escalate gradually.

| Type of Test | Process | Participants | Frequency | Complexity |
|---|---|---|---|---|
| Desk Check | Check the structure and content of the plan | Author of plan | High | Low |
| Walk Through | Discuss the theory of the plan to check that it is usable | Author of plan<br>Users of the plan | | |
| Simulation | Use the plan to undertake a theoretical response to an incident | Facilitator<br>Users of the plan<br>Others as required (e.g. observers) | | |
| Unit Test | Confirm that a recovery procedure or the recovery of a piece of technology works | Users of the procedure or technology<br>Others as required (e.g. technicians) | | |
| Unit Rehearsal | Practice a recovery procedure or the recovery of a piece of technology, following a script | Users of the procedure or technology<br>Others as required (e.g. technicians) | | |
| End-to-End Test | Confirm that the recovery of a complete area of the organization (a business process, product or service or inter-connected technologies) works | Those in the area of the organization, or those that are required for the business process, product or service, or users of the inter-connected technologies<br>Others as required (e.g. technicians) | | |
| Full Rehearsal | Practice the recovery of a complete area of the organization, a business process, product or service or inter-connected technologies, following a script | All those in the area of the organization, or all those that are required for the business process, product or service or all the users of the inter-connected technologies<br>Others as required (e.g. technicians) | Low | High |

## Frequency

The frequency of a BCM Exercise Programme is dependent upon the nature, scale and complexity of the organization. Each member involved in the organization's incident response capability should be involved in an exercise at least every 12 months. Other events which may require an exercise to be scheduled, include:

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

## Cost of Exercise Programmes

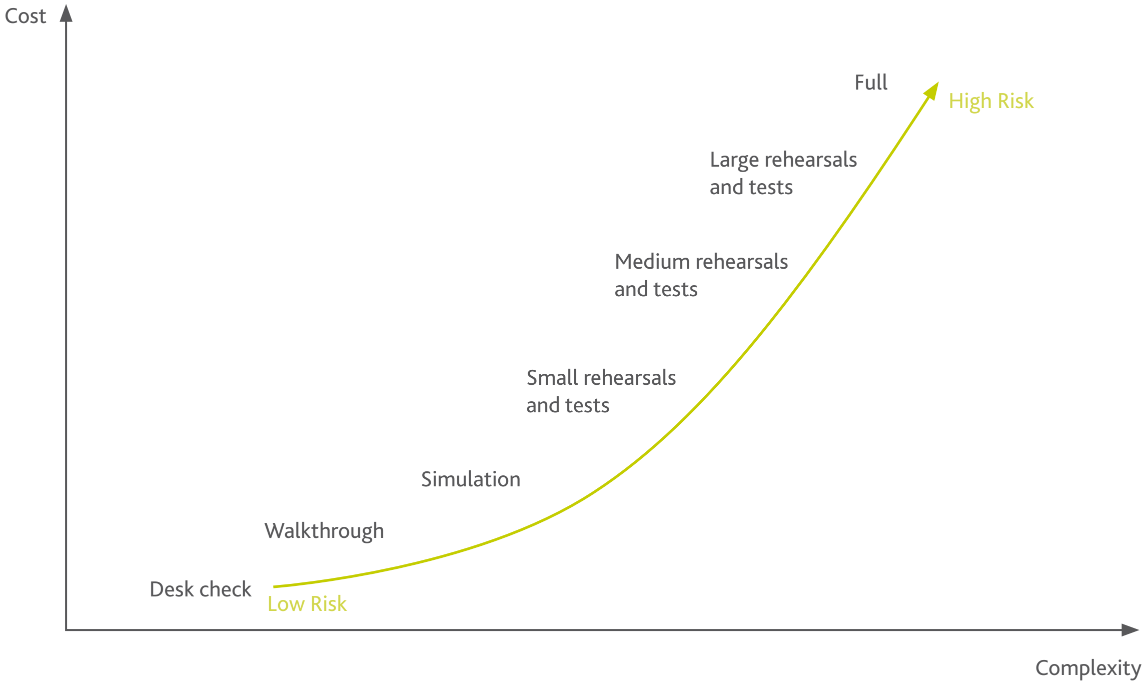
The likely cost of organizing and running an exercise programme is dependent upon the type of exercises selected.

It is important to understand that, as well as increasing cost, increasing complexity in the type of exercise also adds greater risk to an organization.

It is important to recognize that exercise programmes can be costly and in some cases even create additional operational risks to the organization. Clearly small scale exercises such as desk-checks have no real risk of operational interruption and only limited cost implications whereas a full test involving closure of premises and relocation of staff is both expensive to organize and has the potential (should it fail) to leave the business exposed.

The diagram below shows how the cost, complexity and risk are interrelated.

Cost, Complexity, Risk



# Exercising BCM Arrangements

## Introduction

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

1. **Desktop**: Theoretically try out the capability without any actual physical actions being taken. An example is a scenario-based event when decision-making abilities during a major incident are examined
2. **Rehearsal**: The practice of a specific set of procedures or technologies that require physical actions. This is achieved by following a script to impart knowledge and familiarity. An example is a fire drill
3. **Test**: A check to see if a procedure or technology works, where the result can be either a 'pass' or 'fail' (for the procedure or technology, not an individual). It is usually used when the procedure or technology is being tried, often against a target timescale. An example is the rebuilding of a server from back-up tapes within a set number of hours

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.

## Purpose

The purpose of exercising is to:

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

## 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 may require a compromise to be reached between them.

### Stringency

The exercise should feel as real as possible. Tests should be carried out using the same procedures and methods as would be used in a real event. 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. Setting a realistic business scenario helps to ensure that the participants engage fully in the event and ultimately gain more from it. The selection of a feasible scenario will also help prove the viability of plans. It is essential that the exercise facilitator works with facts to ensure that participants gain the most from the exercise through the realism of the scenario and supporting material.

### Minimal Exposure

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

- disruption is minimised

- the risk of something going wrong is understood by Top Management
- the business understands and accepts the risk

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

For desktop or live exercises, the facilitator must have the capability to pause the event if the team is making decisions that would not be appropriate in the scenario.

An agreed Stop code must be arranged in case a real incident occurs during the exercise.

Although it is sometimes necessary to conduct an unannounced test (for example as an out of hours call-out cascade), it is more likely that larger scale exercises are announced to key participants. The warning time given and the number of pre-warned participants will reduce as the organization becomes more confident in its capabilities.

## Outsourcing

Where the delivery of a product or service has been outsourced, the responsibility for exercising remains with the original organization. The organization should make sure, through exercising, that the outsource company is able to deliver its obligations. Other suppliers of time critical materials or activities are identified in the Business Impact Analysis (BIA) and should be asked to demonstrate their recovery capability over their own business and more specifically in relation to the service they provide to the organization. The exercising of outsourced activities should be enforced through a service level agreement (SLA). Care should be taken to review the continuity implications of any “force majeure” clauses in supplier contracts.

## Process

| Technical Test | Scenario Exercise |
|---|---|
| Agree the scope and objectives of the test | Agree the scope and objectives of the exercise with Top Management |
| Agree budget for the test if required | Agree the budget for the test |
| Assign appropriate personnel to the task | Agree with the appropriate managers of the organization and any suppliers of logistics/services required to enable the exercise to take place |
| Devise a simple scenario and set of assumptions that puts the test in context | Prepare a realistic and suitably detailed scenario. Include aspects such as date, time, current workload, political and economic conditions and temporal/seasonal issues<br>Ensure required participants are available |
| Conduct a Risk Assessment of the test to minimize the risk of an impact on live operations | Conduct a Risk Assessment of the exercise to minimise the risk of an impact on live operations<br>Brief observers and prepare questionnaires for use during the exercise to capture lessons learned<br>Pre-exercise information and briefing of participants. |
| Conduct the test and record the results | Conduct the exercise and collate observations |
| Assess and report the results | Debrief participants immediately after the exercise<br>Schedule a date and time for formal debrief |
| Address any issues raised | Use debriefing results to prepare Post Exercise Report and recommendations<br>Prepare an open-issues report during and immediately following the test<br>Circulate reports to participants and Top Management<br>Create an action plan to implement post exercise report recommendations. |

### Methods and Techniques

Participants involved in desktop or scenario exercises may include:

- Facilitator (s)
- Observer (s)
- Suppliers of specialist technical resources and services
- Insurance representatives
- Emergency Services
- Security
- Local Authority Emergency Planning Officer
- Communications and Public Relations
- Subject Matter Experts
- Suppliers of business services/products
- Outsourced service providers

### Outcomes and Review

The outcomes of the BCM exercising process include:

- Validation that the Business Continuity strategies are effective
- Confirmation that team members and staff are familiar with their roles, accountability, responsibilities and authority in response to an incident
- Validation of the technical, logistical, administration aspects of the Business Continuity Plan(s)
- Confirmation of the recovery infrastructure (command centres, work areas, technology and telecommunications resource recovery, etc.)
- Confirmation of the availability of staff and processes for relocation
- Documentation of exercise results in a Post Exercise Report for Top 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 in the BCMS

## Maintaining BCM Arrangements

### Introduction

The BCM Maintenance Programme ensures that the organization remains ready to manage incidents despite the constant changes that all organizations experience. To be effective, the BCM Maintenance Programme should be embedded within the organization's normal management processes rather than be a separate structure that can be ignored or forgotten.

An effective change management process is a prerequisite of maintenance of the BCM programme. Many of the issues that show up in tests and exercises are the result of internal changes within the organization – staff, locations or technology.

### Process

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

The process must include a mechanism to flag and review internal changes to:

- Business processes
- Technology
- Staff
- Products and services
- The legal or regulatory environment

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

Other activities in the process include:

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

### Methods and Techniques

Each plan owner is responsible for updating their plans and dynamic data such as staff out-of-hours contact numbers, team tasks, notification and supplier contact details as well as battle box contents.

Plan sections are updated at frequencies ranging from monthly to annually, in accordance with the schedule in the BCPs Maintenance section. The appropriate update months are also specified in the BCP Maintenance section.

'Date of last update' is to be clearly displayed at the beginning of each plan to provide an effective audit trail.

### Outcomes and Review

The outcomes from the development of the BCM Maintenance Programme include:

- A documented BCM monitoring and maintenance programme
- A clearly defined and documented Maintenance Report (including recommendations) approved by an appropriate Top Manager
- A clearly defined and documented BCM Maintenance Report Action Plan approved by an appropriate Top Manager
- Effective and current BCPs, strategies and solutions

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 BCM Plan Maintenance documentation
- After a real plan invocation, when lessons learned can be incorporated

## Reviewing and Auditing BCM Arrangements

### Introduction

There are several ways to review a BCM programme, which include self-assessment (first party), internal audit (second party) and external audit (third party).

A formal BCM Audit process ensures that an organization has an effective Business Continuity programme.

BCM Audit has five key functions:

1. To validate compliance with the organization's BCM policies and standards
2. To review the organization's BCM solutions
3. To validate the organization's range of BCM plans
4. To verify that appropriate exercise and maintenance activities are taking place
5. To highlight deficiencies and issues, and ensure their resolution

Auditing is designed to verify that the process has been followed correctly, not that the solutions adopted are necessarily correct.

The audit or review should be conducted against a BCM Policy and appropriate standards identified by it.

The audit should be conducted on a regular basis as defined by the organization's audit and governance policies. For BCM, it is recommended that the period between audits should not exceed two years. In the interim, self-auditing, or 'Performance Monitoring' may be carried out more frequently, by the owners of the plans.

The BCM function itself should periodically be subject to a Quality Assurance (QA) process.

## Concepts and Assumptions

This audit approach assumes that if the process is correct and properly applied then the outcome should provide evidence of effective BCM competence and capability. It is also assumed that there are appropriate standards available, which provide a suitable framework for audit. These include:

- National standards e.g. BS25999-1 Code of Practice and BS25999-2 Specification, Singapore Standard SS540, US standard NFPA 1600 and pending standards from Standards Australia and the American Society for Industrial Security (ASIS)
- Regulatory requirements by local financial regulatory authorities, much of which is international in nature and based upon the BCM High Level Principles issued by the Basel Joint Forum for Banking Supervision
- Legislative requirements e.g. the UK Civil Contingencies Act (2004)
- Industry 'Good Practice' guidelines (such as BCI GPG 2010) or those specific to the organization's sector
- Related industry standards e.g. ISO/IEC 27001 (Information Security) and BS25777:2008 (Information and communications technology continuity management)
- An international certification standard for Operational Continuity is also being produced by ISO under the reference code ISO22301, with a supporting code of practice ISO22399 (also in development)

## Process

The BCM audit 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:

- Develop 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, which in part might be driven and governed (or restricted) by legal or regulatory requirements
  > Identification of the standard audit framework to be used (where appropriate). The audit framework may be governed or restricted by legal or regulatory requirements
- Define the audit scope:
  > Determine the corporate governance, compliance or other issues to be audited
  > Determine the area/department/site of the organization to be audited
- Define 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
- Compile and summarize interview notes, questionnaires and other sources
- Identify gaps in content and level of information gathered then conduct further or follow up interviews as appropriate
- Obtain and compare relevant documentation e.g. BIA with interview data and other sources e.g. walkthrough, physical inspection, sampling
- Reference secondary sources e.g. standards, regulations, and 'good practice' guidelines to validate preliminary findings
- Form an opinion that should reflect both the interests of the audit sponsor and the measurements set by external sources e.g. regulatory, legal, industry standard
  > Assigning a risk weighting to individual audit item to distinguish between high, medium and low risk findings
  > Defining criteria for rating factual findings by using a clearly differentiated categorised predefined rating level
- Provide a draft audit opinion report for discussion with key stakeholders

- Provide an agreed audit opinion report incorporating recommendations as well as audited responses where differences of opinion persist
- Provide 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
- Provide 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 QA process includes:

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

## Methods and Techniques

The methods used for audit should be determined by those undertaking the audit and comply with individual organization's policy.

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

- Number of months since last exercise
- Number of open-issues still outstanding since last exercise
- Completeness of the BCM plan documentation
- Number of months since last BIA
- Number of open-issues still outstanding since last BIA
- New IT application assessed for inclusion in BCM Management/Plans
- New or changed business process assessed for inclusion in BCM 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 responsibilities
- Self assessment assurance scorecard

Quality assessment may come from:

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

## Outcomes and Review

The outcomes of a BCM audit include:

- An independent BCM audit opinion report that is agreed and approved by management
- A remedial action plan(s) that is agreed and approved by Top Management
- The outcome of an unfavourable performance rating will be:
  - > Acceptance of the BCM Plans by management as 'inadequate'
  - > The initiation of a BCM review conducted by a BCM 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

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

# Supporting Information

The information on the following pages provides more detailed advice and guidance on various BCM related topics but does not constitute part of the Professional Practices for purposes of BCI membership certification

# ANNEXE 1

## Advice on Selecting Appropriate Tactical Recovery Options

### People

A precursor to identifying and selecting tactical options for the people employed by an organization is to have identified the key skills and knowledge required. This can be done most effectively during the "Understanding the Organization" stage of the BCM process when data about the resources needed is being collected.

The tactical options for the loss or absence of an organization's people include:

- Identifying and documenting details of which people have key skills and knowledge
- Training individuals to acquire additional skills and knowledge
- Documenting key processes to allow staff to undertake roles with which they are unfamiliar
- Keeping a list of retired or ex-employees with key skills and knowledge that can be called up when required
- Using people with the relevant skills and knowledge from a third party (either through a contractual arrangement or keeping a list of suitable third parties)
- Geographical separation of individuals or groups with key skills and knowledge
- Outsourcing a portion of the work requiring key skills and knowledge to a third party that has the capability of taking over more of the work at short notice

### Premises

The choice of options for the loss of or exclusion from premises will be influenced by many factors (some of which may not be known until after the disruption has occurred), including:

- Cost
- RTOs for the affected activities
- Willingness of staff to travel and/or relocate
- Number, size, geographic spread, and nature of the organization's sites
- Willingness to accept increased levels of risk
- Geographic effect of the incident
- Number of staff to be relocated
- Availability of spare space at other sites
- Availability of local vacant premises
- The type and nature of the facilities required at the alternative premises
- The need to access computer systems
- The need for and the availability of communications
- Size and nature of available land around or near to the affected premises

There are no simple guides that can be used for the selection of appropriate options for the loss of premises, although in most cases the options with shorter recovery times cost more than those with longer recovery times. Organizations 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.

The tactical options for the loss of premises include:

- Using available space at another of the organization's sites (this might include meeting rooms, training space, canteens, etc.)
- Increasing staff density at another of the organization's sites (sometimes referred to as 'budge-up')
- Displacing staff undertaking less urgent activities from another of the organization's sites and using the space made available (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 like hotels. Working from home can be a very effective solution but care must be taken to ensure Health and Safety issues are addressed, suitable IT equipment with properly licenced software is provided and sufficient networking capacity/technical support is available
- Reciprocal agreements with other organizations to use their premises – care must be taken when establishing this type of agreement to ensure that testing is allowed and procedures are put in place to ensure that periodic checks are made to determine whether or not the required space is still available
- Using a list of available premises or potential suppliers of premises to find alternative premises after the disruption (this option is suitable for activities with relatively long RTOs, and is often referred to as 'Ad-hoc')
- Contracting with a third party to provide a recovery site

- Acquiring and fitting out additional premises ready to be used when required as a recovery site (this can range from keeping an empty facility that needs fitting out through to having a fully equipped replica site)
- Temporary prefabricated accommodation (caravans, cabins, etc.) – this requires available land that is suitable, can take a number of days to construct, and may require significant preparation of foundations, and other site preparation including the supply of power, water, and telecommunications
- Mobile accommodation – can be brought into use rapidly, but provides limited space and may require service and power connections
- Moving the activity, but not the staff, to another site that has the capability to undertake the activity (known as 'Diverse Locations')
- Replica sites – the activity is transferred to one or more alternate locations, at which staff and facilities are already prepared to handle the workload

This last option is normally amongst the more expensive to implement (due to the costs of synchronising systems and data at multiple sites as well as the overhead of supporting multiple sites and resources), but provides the appropriate solution where quick resumption is necessary. To be a viable recovery option, the sites should have no single points of failure and an appropriate geographical separation.

## Resources

In addition to the options outlined below, asset restoration services are provided by a range of specialist companies who can often minimise damage after fire and flood to papers, books, electronic media, equipment and other assets. These firms may provide an advance registration service and advice, as well as being available on request post incident.

### Resources – Information Technology (IT)

The cost of the tactical options available for the recovery of IT rise significantly in inverse ratio to the RTO (the shorter the RTO the higher the cost). This can often lead to an organization re-appraising the RTOs of its activities (and hence its products and services) once the cost of recovering IT within the desired RTO is understood.

The tactical options available for the loss of IT, which are not mutually exclusive and can be mixed and matched, include:

- **Backups** – backing up the information held in the computer systems, and storing the back-ups in a safe and secure location that is geographically separated from the computer systems on which the original information is held
- **Ad-hoc** – wait until the IT is lost and then obtain replacement equipment if required, and recover the systems and information from back-ups (this option is low cost, but high risk, and is suitable where the RTO is in weeks rather than days, or where the replacement equipment is readily available and the configuration of the IT is relatively straightforward)
- **Support Agreement** – enter into a support agreement with a third party to supply replacement equipment in a pre-defined time period to a pre-defined configuration, and recover the systems and information from back-ups
- **Standby Equipment** – spare equipment held as a standby (either pre-configured or not) that can be used if equipment is lost, with the systems and information recovered from back-ups (holding standby equipment at a geographically separate site will improve the chance that the standby equipment is available when required)
- **Duplicate Equipment** – a complete duplicate of equipment pre-configured with the systems already loaded, that can be used if equipment is lost, with the information recovered from back-ups
- **Third Party Equipment** – a contract with a third party to use their equipment located at a third party site, with the systems and information recovered on to their equipment from back-ups
- **Replica Systems** – replicas of the equipment, systems, and data, which can be held at one of the organization's own sites or at a third party site (a geographically separate site will improve the chance that the replica can be used when required) and can take the form of:
  - > Continuous Replication – where the data is being continually replicated from the original system to the replica (theoretically providing zero data loss)
  - > Mirroring and or Shadowing – where changes to the data in the original system are mirrored or shadowed in the replica (providing minimal data loss)
  - > Logging – where changes to the data in the original system are logged and batched before being sent to the replica (depending on the timescale used, data loss could be measured in minutes or hours)
  - > Backup – where a backup is taken of the data in the original system, which is then copied to the replica (changes made to the original since the last backup would be lost)

The expected lead-time for acquiring equipment in a widespread incident needs to be taken into account when selecting tactical options for IT. This lead time could be long when less-prepared organizations may be chasing the same equipment. Any form of verbal promises by a supplier to keep a contingency stock should be treated as non-contractual.

Terms often used include:

- **Syndicated or Shared Subscription** – a work area is where a subscriber pays for the use of shared accommodation that is provided when not already in use by a prior invocation by another subscriber (this is the lowest cost option, but carries the highest chance that the space may not be available when required)
- **Exclusion Zone** – a type of exclusivity on shared accommodation, where a subscriber may choose to exclude other subscriptions to that work area by geography, and/or industry type. It does not however reduce the risk of sharing ratios with other non-excluded subscribers. (Care is needed not to confuse the above term with an "Incident Exclusion Zone" which is the area from which the public are excluded by emergency services during the response to an incident)
- **Guaranteed** – a work area that offers the subscriber the ability to have a certain percentage of accommodation guaranteed from the total amount subscribed in the event of multiple incident invocations (for example, a subscriber may contract 200 spaces with a guarantee of 25%, which would assure that subscriber 50 spaces in the event of other invocations)
- **Dedicated** – a work area where a subscriber has exclusive use of accommodation. This is the highest cost option and carries the lowest chance that the space may not be available when required, and is generally used where a rapid RTO is required, for high value-generating functions, where specialist equipment is used or where shared space is deemed unacceptable

For shared work areas, the general industry ratio is a maximum of between 10 and 40 to one (i.e. in the higher example each desk is sold a maximum of up to 40 times). The dangers associated with this and the parameters acceptable to an organization should be clearly defined within its strategy and should not be left to individual contract negotiations.

At the current time there are two main methods upon which a recovery supplier will 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

Clearly the availability of "guaranteed" and "dedicated" areas in those same facilities can make multiple invocation seat resource assignment complex and sometimes open to contractual challenge.

It must also be remembered that just because an incident occurs it does not mean that regulatory, statutory or business standards for information management are suspended. Key issues to address if operations are being transferred to a third party site include:

- **Confidentiality** – measures should be taken to ensure that the required level of confidentiality of data is maintained in all circumstances
- **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), and time should be allowed within the RTO to allow data synchronisation and other issues to be resolved in case they hamper user recovery
- **Availability** – ensuring the information is available at the time required to achieve the RTO for the activity using the information (note that there may be statutory requirements for access to documents or data within a specific timescale following enquiries by the public or authorities)

Tactical options for IT need to be reviewed in conjunction with the tactical options for premises and telecommunications to enable users to be given access to the computer systems that they require for the activities being recovered. This is because the lead time for the installation of new telecommunications lines to alternative premises can vary widely and can be anything up to three months in some countries. Many suppliers of such services also provide replacement accommodation for user staff, which is often called Work Area Recovery.

Web-enabling computer applications and the promised benefits of Cloud Computing locating the systems running those applications at sites geographically separated from the locations of the activities using those systems will improve availability. This will enable users that need those applications to undertake activities to be located at any site where there is an Internet connection. However, appropriate measures need to be put in place to ensure the security of the information so that only those authorised can gain access (for example, by the use of a VPN – Virtual Private Network).

### Resources – Telecommunications

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 impacts thoroughly analyzed to ensure minimal disruption and impact.

Tactical options for the loss of telephone communications include:

- Automatic call diversion
- Manual call diversion
- A recorded message asking callers to telephone another number
- Broadcast notification to staff and other stakeholders of alternative numbers to call
- Non-geographic numbers
- Managed network services
- Mobile switchboard
- Use of mobile telephones – although this cannot be relied upon as mobile telephone communications may be switched off, or become over-loaded, following a major incident

Telephones can often be diverted at short notice, and where the RTO for activities that require telephones is measured in days, waiting until after an incident that causes disruption to redirect telephones can be an acceptable option. However, the un-planned redirection of telephony to alternative locations may not be possible within an acceptable timescale, particularly during wide-area events.

Most telecommunications providers will offer, for a charge, a range of flexible planned solutions that will allow instantaneous or rapid redirection of calls from one site to another or more. This option is to be preferred where the RTO for activities that require telephones is measured in hours rather than days, and where the impact of the loss of telephones is large.

Care needs to be taken in redirecting telephone lines to ensure that sufficient capacity to answer the volume of calls is provided (for example, the redirection of a large number of lines used by a busy call centre to a single telephone will means that the majority of calls will not be answered). Also, the logistical problem of handling telephone calls during an interruption, once they have been redirected, needs to be addressed to ensure that the receivers of the diversions are appropriately skilled to handle the calls and peak influx.

Tactical options for the loss of data communications include:

- Duplicate communication lines (it is important to ensure that there are no single points of failure)
- Use of the Internet (for web enabled systems)
- Relocating the staff needing to use the systems to sites that still have working data communications

There has been rapid growth, particularly in Asia, of Business Process Outsourcing (BPO) which normally includes both call centre operations and back office processing. Integration of data and intelligent telephony in an off-shore location can provide significant recovery challenges. BPO based call centres will usually have a contractual and short RTO, so two or more centres geographically dispersed load sharing the calls are often an integral part of the response.

Due to the typical staff make-up of this type of facility, a sustained period of outage can present human resource challenges in the event that people are unwilling or unable to relocate given the long distances involved in some countries. However with the advent of skills based call routing, an event impacting a single location that is part of a campus model will result in calls being diverted to agents with similar skills/knowledge in another location.

### Resources – Paper Information

Many organizations still rely on paper records, and in these cases tactical options for their loss need to be identified and selected.

Tactical options for the recovery from the loss of paper records include:

- Do nothing – accept the loss
- Copy the paper records and store the copies at a site geographically separated from where the original records are held
- Scan the paper records and store the images electronically (the electronic records can be held either at the same site, with backups held elsewhere, or at a geographically separated site)
- Recreate the paper records as best as possible from information supplied by staff, customers, suppliers, and other stakeholders

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 data 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 RTOs are threatened. Some papers may be work-in progress and be required in short timescales. Others may be archived for legal or regulatory purposes for which off-site will be more suitable. When evaluating, it is imperative for the organization to have a clear understanding of their data strategy, policy and compliance/governance imperatives, which can then be aligned and or modified to suit restoration purposes.

The recovery of paper documents following an incident may not be possible, may hamper recovery where it is uncertain what is missing, or may take a considerable time because of damage caused by fire, water, or being scattered following an explosion. Because of this, organizations that rely on paper records should implement measures to protect against their loss. These measures may include the use of fire-proof (or fire-resistant) filing cabinets, safes or vaults, which are only effective for current records if a clear desk policy is implemented. However, even if the contents survive the incident, the cabinets or safes may not be accessible (an example of this situation was seen in the destruction of the World Trade Centre Twin Towers in New York).

In some countries and regions of the world, the original of contractual documents may be the only one legally acceptable.

### Resources – General Equipment

The options for the loss of equipment are similar to those listed above for the loss of IT equipment:

- **Ad-hoc** – wait until the equipment is lost and then obtain replacement equipment if required (this option is low cost and may be suitable where the RTO is in weeks rather than days, or where the replacement equipment is readily available)
- **Support Agreement** – enter into a support agreement with a third party to supply replacement equipment in a pre-defined time period (sometimes referred to as a 'Ship In' contract)
- **Standby Equipment** – spare equipment held as a standby that can be used if equipment is lost (holding standby equipment at a geographically separate site will improve the chance that the standby equipment is available when required)
- **Duplicate Equipment** – a complete duplicate of equipment that can be used if equipment is lost (again, holding such equipment at a geographically separate site will improve the chance that it is available when required)
- **Third Party Equipment** – a contract with a third party to use their equipment located at a third party site

## Special Concerns for Manufacturing

### Production Processes

Specialised equipment is most often found in manufacturing. Unfortunately, few options exist for the loss of specialised equipment because of likely long lead-times on replacement and the fact that such equipment can be relatively expensive, precluding the holding of duplicates.

Options that can be considered include:

- On-site maintenance or maintenance contracts with guaranteed service levels
- Use of subcontractors or competitors with similar equipment configurations
- Holding spares of important components (holding spares at a geographically separate site will improve the chance that they are available when required)
- Holding of older equipment as emergency replacement or for spares (again, holding such equipment at a geographically separate site will improve the chance that it is available when required)
- Changing the process to use more readily available equipment

There are specific issues associated with unique or long lead-time equipment, which include:

- The chance that it is outdated and its replacement may not be possible
- An up to date replacement may require staff to acquire new skills
- An up to date replacement may be incompatible with other equipment, or may require different materials

For multi-national manufacturers, the overall manufacturing base is often viewed strategically as a single capability with a network of linked operational facilities. Consequently geographical diversity – manufacturing the same product at more than one site – increases resilience to a variety of events, but is usually at the expense of economies of scale and might add to distribution and logistics costs.

Subcontracting – although each company's total process may be unique, there are usually various sub-processes that 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 and organizational understanding due to the need for tooling and set-up.

### Materials, Logistics and Inventory

The options for the loss of materials and stock include:

- Storing additional supplies at another location, which could be at the supplier's site, shipping sites or third party recovery sites (but be aware that some materials and stock may degrade over time and need to be rotated with regular stock, or that changes in the process may make the stored materials and stock redundant)
- Arrangements with third parties for delivery of materials and stock at short notice
- Diversion of just-in-time deliveries to other locations
- Transfer of sub-assembly operations to an alternate location either in-house or to a subcontractor

### Power and Utilities

The options for the loss of power include:

- **Uninterruptible Power Supply (UPS)** – to cover short power outages and enable the safe shut down of equipment (particularly computers)
- **Standby back-up generators** – that cut-in, either manually or automatically, when power fails to protect buildings or equipment from more prolonged power failures (however, these need to be maintained and tested regularly to ensure performance when required)
- **Portable generators** – shipped in when required either as a contracted service or on demand (this would be subject to availability, and in the event of a wide spread disruption of power may be difficult or impossible to obtain)

For all manufacturing plants the availability of water supplies both for staff and process purposes will be essential. Other fuels (gas and oil) will also be essential and the suppliers of all utilities need to be involved in the BCM process.

### Resources – Supplies and Suppliers

Options for the loss of suppliers include:

- Dual or multi-sourcing of supplies
- Identification and pre-acceptance of alternative suppliers
- Contractual obligations on the supplier to implement BCM
- Inspection of supplier's BCM capability for the products and services supplied, which should include evidence of successful exercises
- Holding spare or buffer inventories
- Significant penalty clauses on supply contracts (though this will not protect against supplier bankruptcy)

# ANNEXE 2

## Advice on Selecting Alternative Risk Mitigation Measures

For those Products and Services that are deemed out of scope, the business risk of loss or non-availability is not mitigated by use of the BCM Lifecycle model, and has to be managed by alternative means. The choices available to Top Management are:

- Acceptance – accept that it is at risk of being disrupted
- Transfer – transfer the risk of disruption to a third party
- Change, suspend or terminate the product or service

### Acceptance

If the cost of full 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 might be accepted.

In this event the organization 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 a 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 minimizing specific threats in the hope that, if the worst happens, the uniqueness of the organization will permit reinstatement however long this takes

Acceptance of a risk and determination of an organization's risk appetite is subject to the fact that it is not possible to scientifically determine a value for an operational risk, therefore an organization cannot measure this accurately against its theoretical risk appetite. If an organization seeks to protect against specific perceived threats then the overall cost of the measures may exceed that of a Business Continuity strategy.

### 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 organizations are outsourcing business critical processes and activities to create virtual organizations. Transfer of risk is often cited as a reason for outsourcing. It is important to remember that the risk to the organization's reputation and brand image cannot be shifted to either intra-organization sourcing or outsourced providers; the risk and responsibility always remains with the organization
- **Off-shoring** – using in-house resource or outsource providers away from the centre of the business which 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

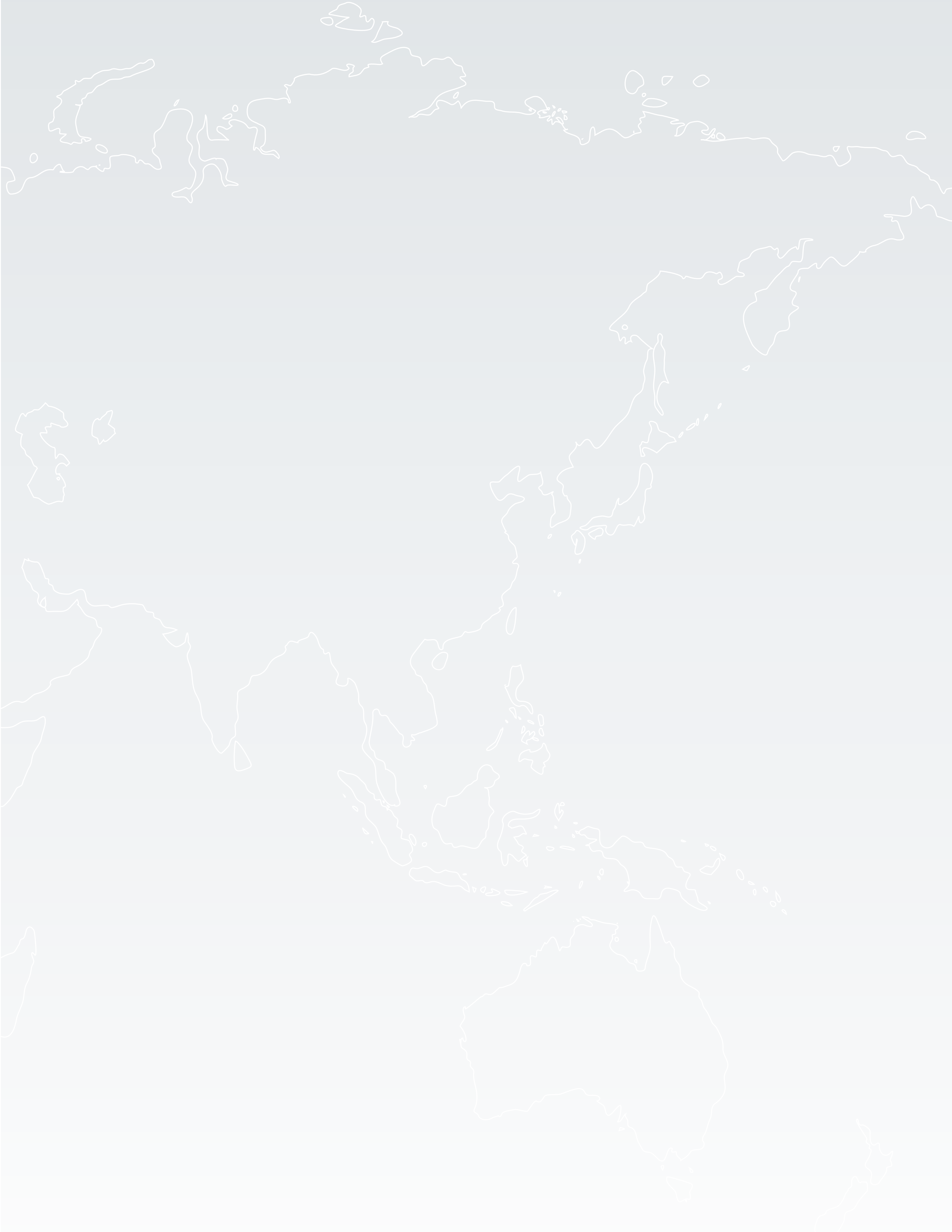
The organization may still suffer damage to its reputation or be liable to penalties as a result of the failure of the company to which they have outsourced.

### 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 reselling under their own label.

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 an organization which is 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 organization faces the threat of possible litigation and reputation damage in the event of a failure to deliver to the customer's expectation.



Business Continuity Institute
10 Southview Park
Marsack Street
Caversham
Berkshire RG4 5AF
United Kingdom