Good Practice Guidelines
2013 Global Edition

A Guide to Global Good Practice in Business Continuity
Contents

Acknowledgments ............................................................................................................. 4

Introduction to the Good Practice Guidelines 2013 ................................................. 5
  Why do we have a GPG?
  What has changed from the GPG 2010?
  Who should read this guide?

The origins of Business Continuity and the BCI .................................................. 6

Frequently asked questions ......................................................................................... 7

The BCM Lifecycle ...................................................................................................... 13

BCI Professional Practices ......................................................................................... 15

Management Practices
  Professional Practice (PP1) – Policy and Programme Management
  Professional Practice (PP2) – Embedding Business Continuity

Technical Practices ...................................................................................................... 47
  Professional Practice (PP3) – Analysis
  Professional Practice (PP4) – Design
  Professional Practice (PP5) – Implementation
  Professional Practice (PP6) – Validation

Glossary of Terms ....................................................................................................... 106
Acknowledgments

These Good Practice Guidelines (GPG) draw upon the considerable academic, technical and practical experiences of the members of the Business Continuity Institute (BCI).

They are intended for use by professionals, consultants, auditors and regulators with a working knowledge of the rationale behind Business Continuity and its fundamental principles. They are not primarily intended to be a beginner’s guide, although they do provide much excellent material for those new to the topic.

It is recommended newcomers should also work alongside an experienced professional or attend appropriate education programmes.

The work on the GPG 2013 commenced in January 2012. The initial drafts were produced by June 2012, with peer reviews, wider consultation and assessments taking place until the end of September 2012. Final consolidated versions were agreed by the Editor in Chief during October 2012 and submitted for review and approval by the BCI Global Membership Council.

Work on translations, examinations and training programme modification took place from November 2012 to February 2013.

The project team responsible for GPG 2013 were:

Editor in Chief: Lyndon Bird FBCI

Assistant Editor: Deborah Higgins MBCI

Contributing Authors: Lyndon Bird FBCI; Ian Charters FBCI; Mel Gosling MBCI; Tim Janes MBCI; James McAlister MBCI; and Charlie Maclean-Bristol MBCI

Administrator: Jan Gilbert

Contributors: Malcolm Brooke MBCI; Jim Burtles (Hon) FBCI; Steven Cvetkovic SBCI; Gianna Detoni MBCI; Stacey Farrow MBCI; Debbie Featherstone MBCI; Lesley Grimes MBCI; Gayle Hedgecock MBCI; Simon Kearney MBCI; David Lightfoot MBCI; Margaret Millett MBCI; Norman Powell MBCI; Keith Prabhu MBCI; Clifford Seow MBCI; Brigitte Theuma MBCI; Pauline Wilson MBCI; John Worthington MBCI; and Anton Wroblewski MBCI.

The BCI acknowledges the time and expertise voluntarily given by all those listed above to the development of this guide for the benefit of the BCI and the Business Continuity global community. It also recognises that this guide would not have been possible without the efforts of many BCI members to the previous editions, so the BCI would also like to thank all those who have contributed in the past. Contributors to these Guidelines have agreed that they have no personal copyright © or Intellectual Property (IP) claim to the material, which is the sole property of the BCI ™.

Lyndon Bird FBCI
Editor in Chief
Technical Development Director, BCI
Introduction to the Good Practice Guidelines 2013

Business Continuity (BC) has changed considerably since the formation of the Business Continuity Institute (BCI) back in 1994 and will continue to evolve as its value is recognised by a wider audience.

BC seems particularly pertinent at this time. The world has still not fully recovered from the global economic crisis of the last decade. We are coming to terms with a new economic and political order as well as trying to deal with increasing global threats, ranging from energy, security, mass migration, cyber-crime and climate change. Against this background, it is encouraging that the discipline of BC has proven to remain relevant in the face of these major business and societal changes.

For those individuals who wish to become Statutory members of the BCI, competence needs to be shown in all six BCI Professional Practices (PP). The Certificate of the BCI Examination (CBCI) tests knowledge of the Good Practice Guidelines subject matter across all Professional Practices. Successful candidates will be awarded a pass or a pass with merit. It is important to fully understand the contents of this guide before attempting the Certificate of the BCI Examination. The BCI Diploma (DBCI) is an academic qualification in Business Continuity leading to the post nominal designation DBCI which can also lead to Statutory Membership of the BCI.

For those wishing to upgrade to Statutory membership levels (AMBCI, MBCI, and FBCI) proven experience will also need to be demonstrated. Details of the experience needed for each level is available at www.thebci.org

ISO 22301:2012 terminology is relevant throughout these Good Practice Guidelines (GPG 2013).

A comprehensive list of all terminology used in these Good Practice Guidelines can be found in the Glossary of Terms.

Why do we have a GPG?

With both national and international standards for Business Continuity (BC) now available, the GPG has changed. The publication is no longer the sole provider of serious subject matter content but it remains the most comprehensive and independent view of current thinking in the subject. The real value to BC professionals is that it considers not just the “what to do” (which standards do cover) but also the “why”, “how” and “when” of practices written by real-world experts. It is not a specification or requirements standard. It aims to enhance and complement emerging standards in Crisis Management, Incident Management, Emergency Planning, Organizational Resilience and Governance, Risk and Compliance (GRC).

This version has been written primarily for BC professionals. It is the current body of knowledge for the profession in terms of how to practise the discipline. Unlike a management system standard, it can have the flexibility to identify future trends,

<table>
<thead>
<tr>
<th>BC</th>
<th>Business Continuity</th>
<th>The capability of the organization to continue delivery of products or services at acceptable redefined levels following a disruptive incident.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
<td>A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.</td>
</tr>
<tr>
<td>BCMS</td>
<td>Business Continuity Management System</td>
<td>Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.</td>
</tr>
</tbody>
</table>

SOURCE: ISO 22301:2012
challenges and issues that professionals are still debating. As such, it provides an accepted benchmark against which the knowledge of professionals can be examined and which can form the basis of academic training.

What has changed from the GPG 2010?

There was no need to change the principles of the GPG substantially, so the main components remain the same but there has been some refinement of language. This version still covers the same six stages of the BCM Lifecycle and links them to what are defined as Professional Practices (PP). The six Professional Practices are sub-divided into two Management Practices and four Technical Practices. It has been decided the naming of the individual PPs should be simplified and the following section headings are used:

### Six Professional Practices (PP)

#### Management Practices

<table>
<thead>
<tr>
<th>PP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP1</td>
<td>Policy &amp; Programme Management</td>
</tr>
<tr>
<td>PP2</td>
<td>Embedding Business Continuity</td>
</tr>
</tbody>
</table>

#### Technical Practices

<table>
<thead>
<tr>
<th>PP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PP3</td>
<td>Analysis</td>
</tr>
<tr>
<td>PP4</td>
<td>Design</td>
</tr>
<tr>
<td>PP5</td>
<td>Implementation</td>
</tr>
<tr>
<td>PP6</td>
<td>Validation</td>
</tr>
</tbody>
</table>

Since the release of the International standard for business continuity management systems ISO 22301:2012 and ISO 22313:2012 the GPG 2013 uses the relevant terminology where appropriate. However, the GPG 2013 recognises a clear difference between Business Continuity (BC) as the wider discipline and Business Continuity Management (BCM) as the management process. In the GPG 2013 the term Business Continuity is used wherever the wider discipline is being discussed but the term Business Continuity Management is used when discussing the management process and activities involved, such as the BCM programme and the BCM Lifecycle.

Who should read this guide?

The GPG is not only for those seeking professional certification. As a body of knowledge the GPG is used as an information source for BC training programmes and awareness campaigns for colleagues who need to understand the subject better. These colleagues may range from crisis communications professionals to supply chain practitioners and human resources specialists.

BC 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.

The use of the term “business” does not mean that BC only refers to commercially-driven organizations: the public sector can also readily benefit from adopting such practices as can the third sector, which incorporates voluntary and not-for-profit organizations. In fact, many voluntary organizations are critical delivery partners to public sector agencies.

While BC can demonstrate healthy adoption among medium-sized and larger organizations, there is a recognised “gap” in adoption among smaller businesses. There is nothing inherently “corporate” about BC; however, the BCI recognises that some small business owners might be unable to follow the GPG completely and simpler alternative materials, grounded in the GPG, will aid them. Such materials will include guidance issued for this purpose by government agencies, other professional bodies and business support groups as well as from the BCI.

The origins of BC and the BCI

In 1993 “Survive” set up a working party to look into the question of training and certification for the BC professional. There was a perceived need to distinguish between the skilled BC professional and the general consultant, usually from an ICT background. Similar debates had taken place slightly earlier in the US and led to the formation of the Disaster Recovery Institute in 1988. This was primarily formed to provide training and certification and emerged from the popular industry periodical “The Disaster Recovery Journal”.

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

Towards the end of the decade, the idea of a holistic end-to-end approach emerged. It was now becoming obvious there was a need to provide protection and resilience spanning 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 other single points of failure. This thinking was already encapsulated in the BC concept first proposed many years before but it had taken more than a decade to gain wide-scale understanding. This made initiatives such as BS 25999 and other national BCM standards more viable as they could be based on a solid conceptual framework.

The 21st century saw a determination to codify BC 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 BS 25999-1 from the UK; NFPA 1600 from the US; and various handbooks from Australia and Asia. Regulatory bodies like the Financial Services Authority (FSA) (UK), Australian Prudential Regulation Authority (APRA) (Australia), and Federal Reserve (US) also became active in this field, particularly after the destruction of the World Trade Centre in 2001 in New York. Formal national standards now exist in a number of countries and since 2012 there has been an ISO requirements standard (ISO 22301) and a separate guidance standard (ISO 22313).

Frequently asked questions

The BCI is often asked to state a position on a number of topics relating to BC and the complementary disciplines. As many of these are still being debated by the BC community, the following points need to be seen as contributing to the debate rather than being treated as a fixed, definitive opinion. The most frequently asked questions are considered below:

What do we use BC for?
There has been a wide-spread perception that BC is just about dealing with large impact, low probability events. It is now more generally appreciated that BC can improve
organizational resilience as part of “business as usual”. The concepts can also be applied to dealing with non-physical events such as supplier failure and business crises arising from adverse media attention.

The successful application of BC 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 to and recover from disruptions. BC 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 prevention measures alone to provide comprehensive protection will inevitably generate misplaced confidence, because most disruptive incidents are by their nature largely unpredictable.

Are BC professionals able to conduct a BCMS Audit? BC professionals are expected to be proficient in all six Professional Practices (PPs), but this does not make them a qualified BCMS auditor which is a professional discipline in its own right with its own institutes and certification bodies.

All BC professionals need to be skilled in exercising, maintaining and reviewing BCM programmes and, as such, they might be required periodically to undertake first party (self-assessment) and second party (peer review) audits. However, additional skills and qualifications are required to undertake a formally recognised third party audit of a BCM programme.

Evidence of a person’s competence to conduct an externally recognised Audit would be the possession of an Audit qualification approved by IRCA (International Register for Certified Auditors) or a similar professional Audit body.

A BCMS audit should not just look at the technical recovery capability of the business but the appropriateness of that capability to the organization’s stated business aims.

Typically these aims could be split into:

- Reputation;
- Supply Chain;
- Information & Communication;
- Sites & Facilities;
- People;
- Finance; and
- Customers.

The use of this simple model will demonstrate to Top Management the value and integrated nature of the approach - cross-functional and enterprise-wide.

Are BC and organizational resilience the same thing? Business Continuity is the discipline that has organizational resilience as its objective. There continue to be attempts to codify organizational resilience as both a discipline and management system in its own right but moving from the academic research on resilience to organizational practice is still very much work in progress. We do not currently see much distinction between Business Continuity as set out in the Good Practice Guidelines and efforts to codify organizational resilience.

Resilient organizations are forward thinking and able to adapt to changing circumstances which may have damaging effects on the organization’s ability to survive. These include such things as changes to the market in which the organization operates, competitors, legislation, technology etc., as well as incidents that disrupt the organization’s ability to deliver its products and services.

Business Continuity helps an organization to build and improve resilience and provides the capability for an effective response to threatening events. As such, BC is one of the key disciplines required in any organization who aims to be a resilient organization.

Do we need a separate crisis management discipline? Crisis Management is the process by which an organization deals with a major event that threatens to damage the organization, interested parties or the general public. This includes events that may not necessarily result in a disruption to the organization’s ability to deliver products and services, but events such as adverse media coverage that might damage an organization’s reputation.
Introduction

Business Continuity Management is defined in ISO 22301:2012 as ‘the process of identifying potential threats to an organization’s business operations’, and as a process ‘which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.’

Crisis Management cannot be considered separately from the discipline of Business Continuity because Business Continuity forms an integral part of building capability to respond to, and recover from situations which are wider than an operational disruption.

**How well do BC and risk management overlap?**

Regardless of the methodology used, most BC professionals would accept the need for the basic principles of risk management. Every organization faces potentially catastrophic threats that are outside of their control, particularly natural disasters such as floods, tsunamis, earthquakes, etc. There may be some physical measures that can be put in place to reduce the likelihood of such events causing major loss, such as installing flood barriers, but the only fundamental way in which these risks can be treated is to take measures to reduce the impact on the organization if the threat occurs. One of the risk treatment options is to take out insurance: however, to be effective this needs to be augmented by a BCM programme. A risk management programme should identify catastrophic threats that are outside of the organization’s control and a BCM programme is one way to reduce the impact of such events.

When an organization implements a BCM programme it will undertake a Business Impact Analysis (BIA). One of the deliverables from the BIA will be an understanding of the activities undertaken by the organization that are the most urgent. These are the activities that would impact the organization the most if they were disrupted. The BCM programme will identify and implement strategies to enable these activities to be recovered before the impact of their disruption becomes intolerable, but it will also identify measures that can be put in place to reduce the chances of the urgent activities being disrupted and it will quantify the resulting impact on the organization.

Risk assessments that are undertaken as part of a BCM programme are usually at an operational level as they are concerned with the disruption of activities. They
can complement the risk assessments undertaken as part of a Risk Management programme, which are often undertaken at an enterprise level. The overlap between BC and Risk Management provides an organization with the opportunity to strengthen its resilience, but this will only happen if the management of the two disciplines is coordinated effectively.

**Can BC fit into a formal risk-based framework?**

Risk Management has existed for many years, with the most widely accepted formal approach being the COSO (Committee of Sponsoring Organizations of The Treadway Commission) model which generally became known as Enterprise Risk Management (ERM).

The COSO model, although popular with the Audit profession, has proven difficult to implement for many organizations and the ISO Standard ISO 31000: 2009 is now seen as an alternative way forward. The COSO model is control driven. It can be described as a risk-based approach to managing an enterprise, integrating concepts of internal control and strategic planning. It attempts to address the needs of various interested parties, who want to understand the broad spectrum of risks facing complex organizations to ensure they are appropriately managed.

Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies using techniques based on this concept.

The ISO 31000:2009 standard is more operational and defines the risk management process as:

• Establishing the risk context;
• Risk identification;
• Risk analysis;
• Risk evaluation; and
• Risk treatment.

Both models define the methods and processes used to manage risks. They provide frameworks for Risk Management although not necessarily detailed techniques. Supporting implementation guides provide more detail on dealing with particular events or circumstances relevant to the organization’s objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises are perceived to protect and create value for interested parties, including owners, employees, customers, regulators and society overall.

This ultimate aim is very similar to that expressed as the main rationale for BC, so clearly the two disciplines must share a number of features. Risk is usually seen as wider in scope than BC, which means that in some large organizations (particularly in the financial sector) BC has to fit into the overall risk framework. This is perfectly possible to accomplish but better sharing of terminology between risk and BC disciplines is needed.

BCM has evolved from IT and disaster recovery, while ERM has its roots in insurance, loss control and compliance.

The original BC concepts were developed at a time when risk managers were mainly concentrating on insurance and so it was necessary to incorporate some limited risk assessment within the BCM programme.
It is important to note that BC is focused on identifying vulnerabilities within organizations linked to the underlying value they support and understanding the impact of their non-availability on the organization. BC is not primarily 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.

Risk managers often see BC simply as a risk treatment for very specific types of operational incidents – usually physical in nature and normally characterised as interruptions to operational activities caused by damage to premises, facilities and technology or shortage of human resources. This is too restrictive in that it defines BC by “what has happened” rather than by “what business consequences need to be managed”.

How can BC contribute to corporate governance?
In the boardroom BC is a key contributor to effective corporate governance. It helps interested parties to ask some searching questions, around:

- The resilience of the company’s business and operating model;
- Key value-creating products and services;
- Key dependencies – priority assets and processes;
- How the company would respond to a loss of or threat to any of these;
- The main threats today and on the horizon; and
- Evidence the continuity plans will work in practice.

What is the difference between BC and Emergency Management?
BC and Emergency Management work together effectively in many organizations, but it requires commitment, planning and regular review. Emergency Management is often seen as part of the incident management plan in a BCM programme.

Traditionally, incident management has been associated with the activation of and liaison with the Emergency Services, whereas emergency management itself has been seen as the domain of “first responder organizations” such as police, fire, ambulance, government agencies and local authorities. Although not universally true, the perception remains that most emergency management is within the public sector, although high physical risk businesses such as oil and gas, chemicals and nuclear will certainly have many highly skilled emergency professionals within their own organizations.

Do international standards change the way we look at BC?
Management system standards, such as ISO 22301, provide an approved process, a set of principles and terminology for a specific subject area or discipline. They provide a technical specification approved by a recognised standardisation body for the repeated or continuous application of a process against which an organization can be measured. They do not explain what an individual needs to learn to become a practitioner in the discipline, how they might go about applying their skills and knowledge, or how an organization might implement BC.

Standards have been created for a large number of disciplines, from Engineering, through Food Safety to Environmental Management, but in none of these disciplines has a standard removed the need for individuals to learn the theory, practice and skills of their chosen discipline so that they can become competent, qualified and skilled professionals. In this regard, BC is no different.

Management system standards are designed for use by organizations and provide a specification against which the organization can be assessed. It does not replace the need for the BC discipline to have a body of knowledge against which professionals can be assessed and neither does it provide instruction in how an organization is to implement BC.

The international standard, ISO 22301, provides an approved process, a set of principles and terminology for a BCMS, which are generally accepted by the BCI. National standards are different. They reflect the particular needs and requirements of individual countries and, as such, the terminology and process may well differ from that of the international standard and the GPG.

Standards therefore, do not reduce or change the need for the GPG. They should be seen as complementary and addressing varying audiences with different purposes and objectives.
How do BCMS standards overlap with other standards?
Management systems provide a formalised method of ensuring that the organization’s programme is effective and aligned to its culture and requirements. Certification of a BCM programme against ISO 22301 or similar standard will require the operation of a management system to be demonstrated.

The management systems approach is used for other disciplines such as Information Security (ISO 27001) and Quality (ISO 9001) and so a Business Continuity Management System (BCMS) (ISO 22301) can be easily added since there is a convergence of such systems around a common standard text.

What is the typical profile of a BC professional?
While veteran practitioners may share backgrounds in ICT, 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 BC 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.

The BC professional 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 BC professional to understand the language, operating model and processes of the organization in which BC is to be applied.

BC is cross-functional by its very nature. The BC professional 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 by these groups.

Those involved in BCM programme will therefore differ from organization to organization reflecting its business and operating model.

Is a dedicated BC professional essential to manage the BCM programme?
In smaller organizations, BC is often seen as an add-on to a multitude of other disciplines including Health & Safety, Security, and IT. However it needs to be acknowledged that this approach could link BC to a specific event or incident type and does not suggest an enterprise-wide approach to BC. It is also difficult for the BC professional embedded within a single function to influence beyond this function. To be effective, therefore, BC must be recognised from the outset by Top Management as a business discipline owned by the business but co-ordinated and facilitated centrally.

During the early phases of implementing BC into an organization, there will be a need for a specialist BC professional function to manage projects, co-ordinate plan developments, organise exercises and tests and validate the BCM programme.

In a more mature organization in which these techniques are embedded at functional level, the role of the BC professional will move to policy setting, governance and quality assurance.

What does a BC professional need to know about horizon scanning?
While it is common practice to consider threats in the Analysis phase of a BCM programme - especially ones which are known to have a high probability in the near-term horizon, and therefore warrant an increased level of preparedness - considering longer term or underlying trends is not as common. This form of horizon scanning can provide an objective perspective on the future development of the BCM programme. For example, the consequences of the globalisation trend can be seen in widespread adoption of extended supply chains, which have introduced new and hidden tiers within the supply chain. Much of this change has happened without the proactive involvement of BC professionals but recent high profile supply chain disruptions have provided an impetus to better understand supply chain vulnerability and extend BCM into the supply chain. Trend analysis may well be performed by strategy or risk management within the organization or by individual lines of business but it is an important resource to tap into and use to ensure the BCM programme is fit for purpose in the near term and in the future.
The BCM Lifecycle: improving organizational resilience.

This BCM Lifecycle shows the stages of activity that an organization moves through and repeats with the overall aim of improving organizational resilience.

**Management Practices**

- **Policy and Programme Management (PP1)** is at the start of the Business Continuity Management (BCM) Lifecycle. It is the Professional Practice that defines the organizational policy relating to Business Continuity (BC) and how that policy will be implemented, controlled and validated through a BCM programme.

- **Embedding BC (PP2)** is the Professional Practice that continually seeks to integrate BC into day-to-day business activities and organizational culture.

**Technical Practices**

- **Analysis (PP3)** is the Professional Practice within the BCM Lifecycle that reviews and assesses an organization in terms of what its objectives are, how it functions and the constraints of the environment in which it operates.

- **Design (PP4)** is the Professional Practice within the BCM Lifecycle that identifies and selects appropriate strategies and tactics to determine how continuity and recovery from disruption will be achieved.

- **Implementation (PP5)** is the Professional Practice within the Business Continuity Management (BCM) Lifecycle that executes the agreed strategies and tactics through the process of developing the Business Continuity Plan (BCP).

- **Validation (PP6)** is the professional practice within the BCM Lifecycle that confirms that the BCM Programme meets the objectives set in the BC Policy and that the organization’s BCP is fit for purpose.

The BCM Lifecycle:

*improving organizational resilience.*
BCI Professional Practices
PP1 - Policy and Programme Management
**Overview**

“Policy and Programme Management” is at the start of the Business Continuity Management (BCM) Lifecycle. It is the Professional Practice that defines the organizational policy relating to Business Continuity (BC) and how that policy will be implemented, controlled and validated through a BCM programme.

<table>
<thead>
<tr>
<th>BCP</th>
<th>Business Continuity Plan</th>
<th>Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
<td>Ongoing management and governance process supported by Top Management and appropriately resourced to implement and maintain Business Continuity Management.</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
<td>Process of analysing activities and the effect that a business disruption might have on them.</td>
</tr>
<tr>
<td>Document</td>
<td></td>
<td>Information and its supporting medium.</td>
</tr>
<tr>
<td>Incident</td>
<td></td>
<td>Situation that might be, or could lead to, a disruption, loss, emergency or crisis.</td>
</tr>
<tr>
<td>Products and services</td>
<td></td>
<td>Beneficial outcomes provided by an organization to its customers, recipients and interested parties.</td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td>Intentions and direction of an organization as formally expressed by its Top Management.</td>
</tr>
<tr>
<td>Organization</td>
<td></td>
<td>Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.</td>
</tr>
<tr>
<td>Outsource</td>
<td></td>
<td>Make an arrangement where an external organization performs part of an organization’s function or process.</td>
</tr>
<tr>
<td>Top Management</td>
<td></td>
<td>Person or group of people who directs and controls an organization at the highest level.</td>
</tr>
</tbody>
</table>

SOURCE: ISO 22301:2012
The Business Continuity Institute (BCI) considers that the BCM programme needs to operate at three different levels:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>Strategic decisions are made and policy is determined;</td>
</tr>
<tr>
<td>Tactical</td>
<td>Operations are co-ordinated and managed; and</td>
</tr>
<tr>
<td>Operational</td>
<td>Activities are undertaken</td>
</tr>
</tbody>
</table>

The BCI recognises that other organizations such as the military and some emergency services might interpret these terms differently, sometimes reversing the operational and tactical levels. Care should therefore be taken in understanding precisely what is meant at each level in these Good Practice Guidelines.

Setting BC Policy

Introduction

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

General Principles

The BC policy of an organization provides the framework around which the BCM programme is designed and built. Organization and governance are essential prerequisites for developing a successful programme. These are set out in the BC policy document, which is owned by Top Management and demonstrates their commitment to it.

The purpose of issuing a policy statement is to communicate to interested parties the principles to which the organization aspires. As its primary purpose is communication, it should be short, clear, precise and to the point. A long complicated BC policy statement will be a barrier to communication.

In many organizations, a high-level assessment of the threats to the organization’s strategic objectives will have been undertaken as part of the business planning process. The output of this can provide a useful input when setting the overall policy for the BCM programme. In some regulated environments, a formal risk assessment is a mandated activity - although the precise methods used are not normally mandated.

Once a BC 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 through a BCM programme.

Process

The process to develop a BC policy is:

- Agree a definition of BC;
- Agree scope;
- Identify and document the components of the BC policy;
- Identify any relevant standards, legislation and regulations that should be included in the BC policy;
- Identify any good practice guidelines or other organizations’ BC policies that could act as a benchmark;
- Review and conduct a gap analysis of the organization’s current BC policy (if it exists) against the external benchmark policy or new BC policy requirements;
- Develop a draft of a new or amended BC policy;
- Review that draft BC policy against organization standards or policies addressing similar and related topics such as quality and security;
- Circulate the draft policy for consultation;
- Amend the draft BC policy, as appropriate, based on consultation feedback;
- Facilitate the sign-off of the BC policy by the organization’s Top Management; and
- Control the distribution of the BC policy using an appropriate version control system.
Determine Programme Scope

Introduction
The BC policy should include the scope of the BCM programme both in terms of what it is designed to protect and the maximum extent of damage, loss or interruption the organization can realistically survive.

General Principles
The purpose of setting the scope is to ensure clarity regarding which 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 fully determined and choices confirmed.

The BCM programme is a continually evolving process, allowing an organization to initially implement a BCM programme in some parts of the organization, while anticipating that it will be extended to the whole of its operations in time. Such an approach overcomes the problems of complexity, cost and scale in implementing a BCM programme in large organizations.

This section spells out the choices available to the organization to protect its delivery of products and services and identifies how and why it might select various products and services for its initial implementation. 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 stages of the BCM Lifecycle. If the organization decides to undertake its initial implementation based on an obvious recovery priority for a specific product or service, it will still need to confirm which activities to include within the initial scope (based on the impact of non-delivery).

Scope is ideally limited by products and services. However location may also be used to limit scope, allowing the BCM programme to include or exclude certain locations and 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

Outcomes and Review

The BC policy will include:

- The organization’s definition of BC;
- A definition of the scope of the BCM programme;
- BC roles and responsibilities;
- An operational framework for the management of the organization’s BCM programme;
- A set of principles, guidelines and minimum standards; and
- Clearly defined budget, audit and governance responsibilities.

While all organizational policies should be reviewed on an on-going basis, as part of BCM programme management, any significant change in the internal or external environment in which the business operates could also trigger a formal review of the BC policy.

In reviewing or auditing a BC policy, the following should be demonstrated:

- Top Management has communicated the policy widely throughout the organization;
- The policy is relevant and suitable for the purpose of the organization;
- The policy clearly states what the BCM programme should achieve;
- There is a clear commitment to satisfy all applicable internal and external requirements; and
- There is clear commitment to ongoing activities and continual improvement.
within the scope. This extends to supporting technologies which have no defined boundaries.

The limitation of scope should be seen as a tactical approach, which allows a staged implementation of the BCM programme across an organization. If a product or service is identified within the scope then all activities that support its delivery must therefore be included.

The documentation of scope for each product and service is intended to explain how the organization intends to protect delivery to its customer. This decision should normally be available for external scrutiny – for example, by customers, auditors or regulators.

Traditionally, organizations have been recommended to plan for the “worst case scenario”. Although this is a desirable objective, it is increasingly clear that for wide-scale natural disasters in particular, there is a scale and scope beyond which recovery is not viable. Beyond that level of interruption, the organization will have to activate a more strategic level business plan to decide upon the feasibility and desirability of continuing business.

For example, a small, single site firm serving a local market would not realistically plan to directly recover from total destruction of both its business premises and the locality in which it operates. However, it would probably have insurance cover and, possibly, other unaffected resources which would allow it to re-start elsewhere if it so decided.

Conversely, a global corporation should be much more operationally resilient, with finance and operational resources available to cope with and recover from major incidents. However, perceived incompetence at dealing effectively with a major crisis can put even the largest organization at risk of collapse.

The scope should be signed off by the Top Management.

**Process**

The process may require the establishment of a steering committee 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 prior Business Impact Analysis (BIA) has been conducted to ascertain the effects of a loss of products and services the group will include the outcome of that work in its review.

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); or
- Telephone support (for a software organization).

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

- A customer requirement;
- A legal or regulatory requirement;
- Perceived high-risk location due to proximity to other industrial premises or physical threats such as flooding; or
- Product generating an overwhelming proportion of organizational income.
Reasons why a product or service may be excluded from the scope include:

- Product/service nearing end of life (and would be terminated if supply interrupted); or
- Product/service with low margins (so it could be terminated or easily 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 interested parties;
- Any reputational damage that may result from an interruption or termination in the supply of a product;
- The relevance of any risk assessment; and
- The impact on regulated activities.

If a particular product or service is included in the BCM programme, it is necessary to put in place suitable measures to ensure that the various activities supporting its delivery can be continued or recovered within the required timescales.

For those products and services that are deemed out of scope, the BCM programme does not mitigate the business risk of loss or unavailability which, therefore, has to be controlled by alternative means.

The choices available to Top Management are:

- Accept there is a risk of disruption;
- Transfer the risk of disruption to a third party; or
- Change, suspend or terminate the product or service.

Top Management must fully understand the implications of these choices, document their decisions and sign-off the decisions as part of the governance process.

Methods and Techniques

Every organization that implements a BCM programme needs to decide on a method to use for determining scope. These can be determined in-house, with reference to a variety of source guidance, including ISO 22301, national standards, regulatory guidelines or relevant legislation and these Good Practice Guidelines.

BCI research has shown that most organizations develop their own method.

The selection or development of a method for selecting scope is an essential part of planning for the implementation of a BCM programme.

The tools that could form part of the organization’s choice of method include:

- Cost benefit analysis (including interested party, legal and regulatory assessment);
- SWOT (strengths/weaknesses/opportunities/threats) analysis;
- Financial planning and management;
- Benchmarking against appropriate national and international standards;
- PESTELO (political, economic, social, technological, environmental, legal, organizational) analysis; and
- Market analysis techniques.

None of these techniques are fundamental skills that a BC professional may possess. Where necessary, they should seek specialist help in using these technical analysis techniques.
Outcomes and Review

The outcome is a scope for the BCM programme, which will be documented in the BC policy.

The review should be carried out at least once every 12 months. However, certain events may prompt re-examination of the scope:

- A BIA revision which identifies substantive changes in processes and priorities; or
- A significant change in one or more of the following:
  - The organization’s attitude to risk (perhaps prompted by an event);
  - Market conditions;
  - Acquisition, merger or disposal;
  - Products or services; and
  - Legal or regulatory requirements.

Defining Governance

Introduction
The BCM programme must be adequately resourced and financed.

Top Management must provide the necessary financial support for the implementation, ongoing management and validation of the BCM programme. Adequate staffing must be made available for successful operation. This is often easier to achieve in regulated industries such as financial services because many regulatory authorities consider that BC is a cost of doing business and make it mandatory.

Top Management must also decide if, or the extent to which, it wishes to adopt formal standards for its BCM programme. This will, in itself, require additional direct funding to achieve the certification and increased budgetary allocation in future years to maintain it. For those organizations that are already familiar with similar systems for Quality Management or Information Security, the decision and the process to be followed will be easier.

General Principles

Management systems provide a formalised method of ensuring the BCM programme is implemented and managed to a recognised standard. In these Guidelines when a formal management system has been implemented, it is referred to as a Business Continuity Management System (BCMS). Certification of a BCM programme against ISO 22301 or any national standard will require the operation of a management system to be demonstrated.

Concepts and assumptions

The management systems approach is used for other disciplines such as Environmental Management Systems (ISO 14001) and Quality (ISO 9001). A BCMS (ISO 22301) can be easily added since there is a convergence of such systems around a common standard text.

A management system for BC can be defined as that part of the overall management system (of the organization) that establishes implements, operates, monitors, reviews, maintains and improves Business Continity.

This requires that the BCMS has:

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

Process

All ISO management systems, including the BCMS, use the Plan-Do-Check-Act (PDCA) cycle.
(See table on the next page for an explanation of the PDCA model as applied to BCMS processes.)
Plan | Establish | Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving Business Continuity in order to deliver results that align with the organization’s overall policies and objectives.

Do | Implement and operate | Implement and operate the Business Continuity policy, controls, processes and procedures.

Check | Monitor and review | Monitor and review performance against Business Continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.

Act | Maintain and improve | Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and Business Continuity policy and objectives.

SOURCE: ISO 22301:2012

Although 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 interested party requirements.

The management system will include the following:

- A documented framework for the BCMS establishing the policy, objectives and scope of the BCMS which will identify the outcomes expected from the BCMS, described in measurable terms. This framework will also establish responsibilities for implementation of the BCM programme;

- A formal management review of BCMS performance against agreed outcomes and assessment of factors, internal and external, which may require changes in the BCMS; and

- Implementation of the results of the review which may include corrective actions to remove non-conformance and measures to improve the effectiveness or efficiency of the BCMS.

Methods and Techniques

The effectiveness of the management system can be demonstrated by:

- Top Management commitment and leadership;

- A formal process for performance measurement;

- 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 in the BCMS;

- Appropriate training of those with roles in programme development and response; and

- Improvement in the effectiveness of the BCMS.

Certification of an organization against a formal standard does not guarantee that it will successfully manage all disruptions, only that it has carried out the aspects of the process of BCMS that can be objectively audited. However,
the rigorous nature of achieving certification does subject an organization to a considerable level of exposure and can build awareness of BC among all levels of the organization.

The organization needs to ensure that Top Management demonstrate positive leadership with respect to BC.

However, it is also essential that other management levels support the BC policy by promoting its importance and relevance to their staff.

This can be accomplished by:

- **Recognising and communicating the need and expectations:**
  - Ensuring the BCM programme is compatible with the strategic direction of the organization;
  - Ensuring the BCM programme achieves its expected outcomes and requirements;
  - Communicating the importance of effective business continuity management and conforming to the BC policy;
  - Requiring reports on programme milestones and feedback on any missed dates;

- **Mobilising support:**
  - Motivating and empowering persons to contribute to the effectiveness of the BCM programme;
  - Providing the resources to establish, implement, operate, monitor, review and improve the BCM programme;
  - Directing and supporting continual improvement of the BCM programme; and

- **Providing direction and guidance:**
  - Integrating the BCM programme requirements into the organization’s business processes.

For organizations that wish to be certified against a standard or who need to have their BCM programme independently audited by qualified external auditors such as regulators, Top Management will need to provide evidence of its commitment to BC.

Methods that demonstrate this include:

- Establishing a formal BCM Programme within the organization which covers implementation, operation, review, maintenance and continual improvement;
- Establishing and communicating a BC policy;
- Personally checking that BC Policy and the Business Continuity Plan (BCP) is validated;
- Establishing roles, responsibilities and individual competences for BC;
- Appointing of one or more persons to be responsible for BC with the appropriate authority for the implementation and maintenance of the programme;
- Ensuring that the responsibilities and authorities for relevant roles are understood and communicated throughout the organization;
- Defining the basis for acceptable level of risk taking;
- Actively involving senior executives in exercising of the BCP; and
- Enforcing internal audits of the BCM programme and acting upon the recommendations to achieve continual improvement.
Outcomes and Review

An organization will require adequate formal controls to be in place to sustain an effective BCM programme.

A key method for establishing control is the development of an audit programme, which is discussed in detail in the Validation stage.

To accomplish this, the organization’s Top Management shall agree:

- What needs to be measured and monitored;
- How this will be achieved;
- The methods for monitoring, measurement, analysis and evaluation;
- When the monitoring and measuring shall be performed; and
- When the analysis and evaluation of monitoring and measurement results shall be performed.

It is essential Top Management are fully involved with and regularly updated about the performance and the effectiveness of the BCM programme. It is also vital they promptly address the lessons learned and weaknesses identified.

This requires that they:

- Act to address adverse performance trends against programme objectives;
- Monitor programme effectiveness to reduce the chance of adverse results occurring; and
- Retain relevant documented information as evidence of the results.

Implementing a BCM Programme

Introduction

The BCM Programme is an ongoing process and needs to be actively managed. The initial aim of this stage will be to successfully complete an implementation of BC, but the long-term goal of the BCM programme is to improve organizational resilience.

General Principles

The early implementation of BC will benefit from a project management approach, but, as it matures within an organization, programme management skills are required to ensure preparedness remains current.

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

An important success factor is the appointment of competent persons to oversee and manage the BCM programme. External assistance from consultants with appropriate 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 choice of which activities to include in a BCM programme, and in what order, will depend on the existing culture of the organization. The only definite rule is that major decisions on continuity options and recovery strategy should not be made until a comprehensive BIA has been undertaken, with the results agreed and signed off by Top Management.
The process of implementing a BCM programme in an organization consists of:

- An initiation process;
- The planning, co-ordination and implementation of projects to undertake initial implementations of the BCM programme;
- Maintaining the levels of awareness; and
- BCM programme management.

The initiation process should be constructed from activities described elsewhere in these Guidelines.

These activities 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 BCM programme;
- Development of a draft BC policy;
- Data collection and continuity options selection;
- Measures to mitigate specific perceived threats; and
- Creation of incident management procedures.

The methods and techniques

Implementing a BCM programme involves managing a number of related projects and the co-ordination of a range of activities.

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

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

Project management techniques are useful for the planning, co-ordination and implementation of projects. Progress should be monitored and corrective actions taken to ensure continual improvement.

Outcomes and Review

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

- An improved level of resilience – which can be demonstrated by a desktop exercise of the incident management procedures; and
- Procedures, structures and skills to maintain and develop the BCM programme.

Reviewing the BCM programme and reporting on a regular basis to Top Management is essential.

Assigning roles and responsibilities

Introduction

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

General Principles

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.

Top Management should assign the responsibility and authority for ensuring that appropriate procedures are adopted and properly implemented in accordance with the requirements of the BC policy. Top Management should also ensure these responsibilities and authorities for relevant roles are communicated to the entire organization.
Top Management should empower individuals to carry out their responsibilities within the agreed reporting policies of the organization. Should the individuals be given this role in addition to their normal activity, the new responsibility has to be added to their job description. These responsibilities should be made known to all interested parties as appropriate. Performance reporting on the BCM programme on a regular basis to Top Management is essential.

Concepts and Assumptions
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 personality characteristics required of planners and leaders are often contradictory. Any difficulties in this area should be exposed by a realistic set of plan exercises.

Nevertheless, those who have been involved in implementing the BCM programme should provide support during incident response. BC professionals should maintain a state of readiness to assist designated incident managers 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 senior member of the organization should be given overall accountability for organizational resilience and its effectiveness. This ensures 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. Depending on the size of the organization, this may be a full or part time role.

Specific skills for those managing the BCM programme include:

- A good standard of education and/or proven experience in a relevant subject;
- Proven ability to identify and analyse problems and develop workable solutions;
- Effective communication and interpersonal skills to work with all levels of an organization;
- Programme management – including project management skills and budget management;
- Analytical skills to undertake a BIA – data collection, design and interview techniques;
- Planning skills to develop and implement plans;
- Facilitation skills to manage and execute an exercise programme;
- Training skills to impart knowledge to BC departmental representatives; and
- Negotiating and influencing skills to gain Top Management commitment.

For larger organizations, additional staff may be nominated to support the BC professional to:

- Act as BC departmental representative in their areas;
- Collect information for the BIA;
- Develop, implement and maintain plans;
- Conduct exercises;
- Undertake document revisions;
- Assist in BC training and awareness activities; and
- Assist with managing incidents.
Additional groups may be formed to assist in the development of the BCM programme. These could include:

- BCM programme board or steering committee – a management group to give advice, guidance and management oversight;

- Strategic, tactical and operational level teams that would respond in an incident and which should contribute significantly to the plans.

**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 BC professionals engaged 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 (BCI). Individual BC professional certification provides assurance of knowledge, credibility and experience.

To ensure BC related 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 both the individuals and the organization.

The level and competence of staff assigned to BC related roles should be reviewed annually as part of the normal budgeting process and may be a topic for their annual appraisal and the subject of an audit.

**Project Management**

**Introduction**

When undertaking an initial implementation of a BCM programme in an organization, project management techniques can be adopted. The project management method selected should be appropriate to the nature, scale and complexity of the organization and its implementation of BC.

**General Principles**

This paves the way towards programme management once the key elements are in place. However, this remains a useful discipline for elements of a BCM programme that have clear deliverables (for example, in rolling out an awareness campaign across the organization).

While a clear deliverable can be identified for some 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
The project management techniques if being adopted should be defined and documented at the outset of the BCM programme.

These Guidelines can be used to identify the projects required to complete an initial implementation of the BCM programme.

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;
- Resources;
- Deliverables; and
- Milestones.

Methods and Techniques
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 an exercise programme;
- Developing and delivering a training programme to staff; and
- Selecting a supplier.

Outcomes and Review
The outcome of the project management method used is the successful delivery of the BCM Programme, within agreed timescales and budgets.

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

Programme Management

Introduction
Once implemented, the BCM programme needs to be managed in a cycle of continual 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 and according to the principles contained in the organization’s BC policy document.

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

In smaller organizations BCM programme management 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 BC responsibilities. In the latter case, staff management skills may be required by those managing the BCM programme.
Policy and Programme Management

Process
The appointed BC professional or team should (in consultation with the Top Management):

- Develop and approve a BCM programme;
- Determine the key approaches to each stage of the BCM Lifecycle;
- Undertake or manage the appropriate activities within the organization;
- Promote BC across the organization and externally where appropriate;
- Manage the BCM programme budget;
- Maintain the BCM programme documentation;
- Ascertain the level of resilience required by legislation and regulation within the relevant sector; and
- Report to Top Management on a regular basis highlighting where there are identified issues.

The appointed BC professional or team may (in consultation with Top Management) identify and train individuals to:

- Act as the departmental representative for any BC related issues affecting the department or location;
- Assist the department to identify and communicate the implications of process change; and
- Assist or lead the department 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 Good Practice Guidelines;
- Assistance from external BC professional;
- A self-assessment against a standard, legislation or regulation;
- Annual personal performance measurement;
- Supplier and outsource provider relationship management;
- Supplier relationship management of BC related specialist resources and services;
- Financial management;
- Legal, statutory and regulatory advice
- Industry sector benchmarking;
- International or national standards;
- Internal and/or independent audits; and
- Review and challenge.
Outcomes and Review

The outcome is the continual improvement of organizational resilience.

Review will include the need to have the following in place:

- A clearly defined and documented BCM programme that is agreed by the organization’s Top Management;
- Reports at a predetermined frequency;
- Clearly defined and documented BC strategy;
- A management process that is an integral part of the organization’s BCM programme;
- The BCM programme annual budget;
- The BCM programme audit report;
- The provision and maintenance of effective competence and capability; and
- Incorporation of lessons learned from real incidents or exercises.

An organization’s BCM programme should be regularly reviewed by internal or external audit.

Managing outsourced activities

Introduction

Where the organization uses methods such as off-shoring (provision of services such as call centres in regions of the world that are remote from the primary client base) or outsourcing back office business processes to deliver important operational activities, it is important that the BCM programme covers these activities.

General Principles

Although similar to the more general issue of supply chain continuity, outsourcers often play an integral role in delivering day-to-day operations.
**Process**

The processes for reviewing the BCM programme of an outsourcing organization are similar to those employed for reviewing the organization’s own.

It is important that access to any relevant information is available for assessing, including:

- Tenders from prospective outsourcers; and
- Ongoing adequacy of arrangements of existing outsourcing companies.

Reliability of outsourcing arrangements may be increased by:

- Prequalification of candidate outsourcing companies;
- Specification of requirements in tender documentation and contract terms;
- Realistic service level agreement for use during incidents at either organization; and
- Involving outsourcing companies in training, awareness and exercising.

**Outcomes and Review**

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

The review of a potential outsourcing partner’s BCM programme should form a significant part of the assessment of tenders when contracts are being awarded or renewed. Annual review of outsourcer’s performance against requirements is recommended.

**Managing Supply Chain Continuity**

**Introduction**

Supply chain continuity overlaps with outsourcing but here it is taken to refer to the large number of suppliers of goods and services on which the organization depends but whose providers do not go through the same high profile and rigorous scrutiny that would be undertaken before a major outsourcing contract was awarded.

**Such supplies include:**

- Utilities – power, gas, oil, telecommunications;
- Raw materials – for manufacturing;
- Office supplies – standard and special stationery; and
- Services – security, transport, maintenance.

**General Principles**

As with outsourcing, the responsibility for business continuity remains with the organization; interested parties will expect the suppliers to be scrutinised before the contract is awarded. The impact of a disruption to a suppliers may therefore cause the organization both financial and reputational damage. Supply disruption often originates below the immediate, tier one supplier and this provides a requirement to ensure each supplier to the organization has also considered supply chain continuity in its own BCM programme.
Organizations should consider the consequences of supply chain failure in their own BCM programme and it could be referenced in the BC policy.

**Concepts and assumptions**
The dependencies of activities on suppliers should be identified during the BIA process. Those that are common to many activities, such as power and telecommunications, will usually be addressed at a tactical level, whereas many other suppliers are managed at the activity level by the responsible department.

Traditionally, supply chain professionals have concentrated on the financial aspects of supply such as the level of spending with a particular supplier. BC tends to focus on the timescale of the impacts caused by an interruption since even a small supplier (in financial terms) can have a rapid and disproportionate effect on overall operations.

**Process**
The recommended process for managing supply chain continuity should include these steps:

- Identify the suppliers for each activity (except for those common to all/most activities);
- Match those to the recovery time required by the appropriate activity;
- Select an appropriate strategy that provides for recovery within this timeframe; and
- Examine the BCP of suppliers for the most urgent supplies or those with a long lead time.

**Methods and Techniques**
The priority set for suppliers and supply chains may take the following into account:

- Financial impact of supply interruption over time;
- Reputational impact of interruption over time; and
- Failure of regulatory compliance caused by interruption.

**Mitigation strategies available include:**

- Dual or multiple sourcing (ensuring at least the second tier suppliers are different);
- Evaluating supplier’s BCM programme;
- Contract penalties (although these may be ineffective);
- Stockpiling;
- Using substitute supplies; and
- Identifying and authorising alternative suppliers.

The strategies selected to protect the supply chain may depend on:

- Availability of alternative suppliers;
- Time in which an alternative supplier can deliver;
- Location of suppliers;
- Nature of product/service supplied;
- Interdependencies with other suppliers; and
- The costs of the alternative strategies.
To assess the BCM programme of a supplier the following should be obtained from them:

- Their procedures for monitoring their programme;
- Their performance metrics appropriate to the needs of you (the customer) not them (the supplier);
- Information on how their BC policy, objectives and targets are to be met;
- Information on how priorities between products and services and other customers have been defined;
- Evidence of compliance with a recognised standard; and
- Historical evidence of problems or successes with managing incidents.

To provide additional confidence in a supplier, the following might be used:

- Direct involvement with tests and exercises;
- Joint management meetings to review issues and concerns;
- Formal performance evaluations;
- Service level agreement flexibility to follow wide-scale disasters; and
- Legal access to records and reports on previous incidents.

Managing Documentation

Introduction
An important part of the BCM programme is to manage the documentation. The documentation needs to be consistent, easy to understand and practical to use. The level and type of documentation should be appropriate to the nature, scale and complexity of the organization.

General Principles
Although documentation of the BCM programme is always important, it has particular significance for organizations wishing to be certified against BCMS 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 documentation fits with the requirement of those standards.

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

Concepts and Assumptions

BCM programme documentation has three purposes:

1. To enable a prompt and effective response to an incident;
2. To help manage the BCM programme effectively; and
3. To demonstrate the effective management of the programme.

Outcomes and Review

Supply chain management should deliver a secure supply chain that can manage any disruption to supplies without unacceptable disruption to delivery of the organization’s products and services.

Supply chain management arrangements should be reviewed when there are significant changes in the organization and at the tendering, contract issue and renewal stages of priority contracts.

Although it is important to maintain BCM programme documentation, its presence on its own is not proof of an organization’s 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 administration.
Methods and Techniques
BCM programme documentation tools include word processing, spreadsheets, flowcharting tools, project management software and databases, or the use of specialist proprietary software. It can also be used to ensure current copies of documents are available at the organization’s various sites. Specialist software may offer some advantages, such as assistance with BCM programme maintenance, but may incur ongoing licence, maintenance and training costs.

A document control system should be established to manage and facilitate:

- Usability and accessibility;
- Approval;
- Update and review;
- Version control;
- Distribution control; and
- Archiving or destruction of obsolete documents.

Outcomes and Review
BCM programme documentation may include the following:

- BC policy;
- Roles, responsibilities, authorities and resources;
- Definitions for BC related projects;
- Progress reports for BC related projects;
- Training and competency records;
- The outputs from BIAs;
- Threat assessments;
- Papers supporting the choice of strategies adopted;
- Incident response structure;
- Incident management plans;
- Strategic, Tactical and Operational level 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; and
- 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.
Practical Implementation Considerations

Introduction
Policy and Programme Management (PPM) is, by its very definition, concerned with the strategic and tactical issues of implementing BC. The operational activities that need to be undertaken to implement BC will be identified through project management for the initial implementation and thereafter through BCM programme management and are detailed in the other sections of the GPG. However, before these activities can be undertaken there are some operational issues that need to be considered.

Concepts and Assumptions
Each organization will need to decide how it intends to undertake the activities that have been identified as being required for their implementation of BC. This can range from a set of basic guidelines to a formal methodology, based on the standards that have been identified in the BC policy.

Method and Techniques
Implementation of the BCM programme may require the following:

- Record the data captured;
- Produce documentation;
- Manage documentation;
- Produce reports; and
- Manage the work.

Tools to support the implementation of a BCM programme can include:

- Office software (word processing, spreadsheets and simple databases);
- Customised software solutions;
- Commercially available BC software;
- Document management systems;
- Automated call out software; and
- Incident management software.
BCI Professional Practices

PP2 - Embedding Business Continuity
Overview
Embedding Business Continuity is one of the ongoing activities resulting from the BCM Policy and Programme management stage of the BCM Lifecycle. This Professional Practice continually seeks to integrate BC into day-to-day business activities and organizational culture. This activity is not unique to BC; other disciplines also need to be embedded in the organization in a similar way.

Disciplines such as Quality, Health and Safety, Environmental Services, Security and Risk Management have similar challenges. So the opportunity to share experience and learning opportunities across various related disciplines is important.

General Principles
The established view of organizational culture is often stated 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, taken together, they create the way an organization views itself, its place in its market and the environment in which it operates.

Measuring these underlying attitudes 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.

Organizational culture
Introduction
The successful establishment of BC within the organization depends on its integration with the organization’s strategic and day-to-day management as well as its alignment with business priorities and organizational culture.

Concepts and Assumptions
The successful implementation of a sustainable BCM programme and the effectiveness of the response to an incident may depend on changing the culture of the organization.

Although attitudes may appear relatively easily changed, when under pressure people may revert to behaviours based on their beliefs even if they conflict with the attitudes that have been nurtured. Behaviour shapes attitudes and over a period of time solidifies into beliefs.

To gain maximum benefit from the BCM programme, it is necessary to ensure BC is seen as an integral part of the way things are normally done rather than as a separate activity.

It is also important to ensure that individuals accept that BC is part of their responsibility and not just something done by BC professionals.
Process
In developing a culture of BC awareness, the following should be addressed:

- The attitudes that “It will never happen here” or “We can cope”. These are particular barriers to embedding BC;
- The willingness of individuals to undertake BC related tasks, such as maintaining plans, in addition to their normal roles;
- The assessment of BC related activities of interested parties including customers;
- The inclusion of BC related concepts in planning and decision-making;
- The performance of staff and management during an incident; and
- The willingness of staff to take responsibility for risk mitigation and incident response.

Conveying knowledge of BC is a straightforward task provided it is effectively communicated and is seen to be having demonstrable benefits to the business or, better still, the individual. However, knowledge is not always enough to persuade individuals of the value of BC.

To influence attitudes and behaviour significantly, a more intensive approach is required. A BC exercise, for example, may change the attitudes of individuals such that the group’s beliefs are changed. The most powerful ways to change attitudes and behaviour are to look at the consequences of action (or inaction) and make it relevant to a person’s short-term aims.

Behavioural change initiatives usually fail to attract lasting commitment unless attitudes and beliefs are also engaged. However, there is a limit to which any initiative can influence and alter the culture of an organization, which will be strongly influenced by the tone set by Top Management. Many organizations have tactical and operational aspects of BC in place but have not necessarily embedded them in their cultural framework. In these situations it is important to concentrate on how staff and management view BC to try to find ways to better channel their commitment to its growth and significance.

Methods and Techniques
The BC professional has a number of approaches available to help develop a BC aware culture within an organization. These are:

- Supporting and encouraging Top Management;
- Embedding the BCM Programme in the day-to-day operation of the organization; and
- Developing competence – through training, education and awareness.

The organization’s level of competence and awareness will change as:

- Individual managers’ responsibilities change;
- Business processes are modified;
- Employee changes occur; and
- Unexpected external and internal events occur.

Factors for success in developing the required attitudes and behaviours include:

- Visible and continued leadership by Top Management. This should include an adequate budget to support the BCM programme. 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 in developing the BCM programme. 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; and
- Focusing on the business priorities of the organization by addressing any corporate or individual issues and concerns.
Leadership of the BCM programme by Top Management is essential for success which they will demonstrate by:

- Ensuring the BCM programme is matched to the organization’s strategic direction and objectives;
- Directing that BC is integrated into business processes;
- Assigning the required resources to develop and maintain the BCM programme;
- Maintaining regular oversight of the BCM programme’s effectiveness; and
- Communicating the importance of BC to staff and other interested parties.

Evidence of this leadership should be in:

- The BC policy – signed by a member of Top Management;
- A strategic Business Impact Analysis (BIA) – agreed by Top Management;
- The agreeing of roles, responsibilities and competencies for the BCM programme;
- Appointments of appropriate personnel to those roles and acceptance of a training programme to develop and maintain those competencies;
- Active involvement by Top Management in BCM programme activities, such as reviews, training and exercises; and
- Reports of audits and reviews of the BCM programme.

The BC professional should recognise that Top Management may not have the time or knowledge to undertake this leadership role unaided and, therefore, should support them through:

- Preparing materials and reports for Top Management;
- Drafting key documents such as the BC policy, strategic BIA and relevant communications for Top Management approval;
- Co-ordinating programme activities around the availability of Top Management; and
- Developing competence specifications and recommending appropriate personnel.

Different organizations have different levels of resilience, sometimes through choice and sometimes through the nature of their particular business model. Research has shown that organizations objectively confirmed as “high reliability organizations” usually share the following characteristics:

- Pre-occupation with avoiding failure;
- Top-level sensitivity to operational activities;
- Wide-scale commitment to resilience in all areas; and
- Deference to expertise, rather than imposed authority.

BC professionals should attempt to encourage organizations to focus on these characteristics. If these are already embedded, then BC itself becomes “the way things are done around here”.

For organizations that are less mature in their commitment to resilience there are still effective ways in which BC can be integrated with other regular business activities. For example:

- Making BC a Top Management agenda item when the organization’s strategic plan is being finalised. This ensures a review of the strategic BIA takes place at the same time;
- Making BC a standing item on management meeting agendas;
- Incorporating BC plans into standard operating procedures;
- Including BC awareness sessions in staff training or induction processes;
- Scheduling BC exercises to coincide with planned shutdowns or quieter business periods; and
- Ensuring new products or services are not launched without full consideration of BC as part of the approval process.
In order to be able to integrate BC into other regular business activities, the BC professional requires:

• Experience and knowledge of business procedures and documentation; and

• Influence in the organization to ensure required actions are carried out.

Outcomes and Review
The outcomes of an embedding process are difficult to measure but nonetheless the targets are important to achieve. They could be measured in terms of:

• Improved leadership, management or performance of the BCM programme;

• Greater confidence by interested parties, especially staff and customers, in the organization’s ability to handle disruptions effectively;

• An improvement in organizational resilience;

• A reduction in the impact and likelihood of disruptions (either actual or potential); and

• Improvement in efficiency of business processes.

Skills and Competence

Introduction
It is essential that all individuals undertaking BC related tasks at any level have the appropriate level of competence for the role. Competence can be achieved by firstly understanding the skills required for the role, and then by providing the necessary opportunities for individuals to obtain these skills. These are provided through:

• Training;

• Knowledge; and

• Experience.

General Principles
All staff should have an awareness of the BCM programme and their role in it. Individuals assigned to undertake specific roles within the BCM programme should have the appropriate competence in the skills to undertake their assigned tasks.

It may be appropriate for some roles to measure competence with a recognised certification in the required skills. It may also be appropriate to include the appraisal of these skills in the individual’s annual review and for this to be recognised in the role’s reward or incentive structure.

Concepts and Assumptions
General training and awareness in BC related issues should be provided for all staff, so that they are able to:

• Recognise an incident;

• Alert emergency responders as appropriate;

• Escalate to the incident management team;

• Respond appropriately to specific threats;

• Respond appropriately when evacuated from the site;

• Understand relevant plans and their role in them; and

• Find out further information about the organization’s BCM programme.

When dealing with an incident there are additional skills that may be required in an organization that are not part of the specific skills of a BC professional, these may include:

• Emergency evacuation direction and security;

• Welfare and first-aid;

• Crisis management;

• Information technology (IT) service continuity and disaster recovery;

• Damage assessment, asset salvage and equipment restoration; and

• Incident leadership and decision-making.
The assessment of skills and competence should extend to all contractors who work at the organization’s site or who provide incident related services.

Consideration should be given to what extent the awareness of the BCM programme should be shared with the organization’s suppliers, customers, contractors and other interested parties, which can generate confidence and reassurance.

**Methods and Techniques**

The following approaches can be taken to develop skills and competence:

- Increasing knowledge through an awareness campaign that supports the achievement of the required level of competence; and

An awareness campaign may include:

- Distribution of e-bulletins, posters, newsletters, dedicated website and other communications;
- Participation in workshops, seminars, presentations, webinars and exercises;
- Attendance at external events such as conferences, local BCI forum meetings or local BC related events;
- Participation in Business Continuity Awareness Week (BCAW) activities; and
- Participation in BC exercises.

Develop a training programme that is aimed at ensuring that individuals are able to attain and maintain the required level of competence.

A training programme may include:

- Classroom-based, instructor led training – internal or external;
- Online training;
- Presentations at team meetings or to Top Management;
- Inclusion of BC subject matter at internal training events; and
- BC exercises.

Prior to undertaking a training programme, a training needs analysis may be justified which comprises three principal tasks:

- Establishing the current level of awareness or competence;
-Specifying the desired level of awareness or competence and how this will be measured; and
- Identifying the nature and scope of the “training gap” to be bridged by the training programme.

Each activity requires appropriate preparation, delivery and follow-up evaluation. Particular attention should be paid to engaging the interest of participants through the use of appropriate media.

Each of these activities will have resource requirements such as:

- Planning and preparation;
- Personnel;
- Accommodation;
- Equipment; and
- Expenses.

These need to be noted and any conflicts of availability resolved. This includes ensuring that resources are not overstretched.
Embedding Business Continuity

**Process**
Designing and delivering a training programme or awareness campaign comprises four principal activities:

**Design**
- Identify the audiences;
- Identify and prioritise the topics to be addressed and defining success criteria; and
- Select the most appropriate delivery methods.

**Planning**
- Discuss and agree the proposed activity at the appropriate level of management;
- Pilot key elements of the training programme and awareness campaign with a selection of staff; and
- Schedule events around staff and resource availability.

**Delivery**
- Deliver the activities according to an agreed schedule.

**Follow-up**
- Measure the effectiveness of the training programme and awareness campaign against the agreed success criteria at completion. The effectiveness should be quantified, wherever possible;
- Periodically assess awareness and competence levels; and
- Redesign material where necessary for continual improvement.

Internal and external events may also lead to an increase in awareness and knowledge of BC. As these can fade quickly from memory, the BC professional should be ready to seize on and develop these opportunities when they arise.

**Managing a Training Programme**
For each role in the BCM programme, the necessary skills and desired competence levels should be identified. The individual assigned can then be assessed according to their current level of competence in their role and any training needs identified. This may include:

- No training required (the person is fit for role at the desired level of competence);
- Some training needed;
- Extensive training required;
- Recruitment of experienced person required; or
- Skill can be provided by third party contractor.
Training can then be arranged for each individual or team. This may include:

• Internal training;
• Self-study;
• External training;
• Mentoring;
• Conferences and seminars;
• Academic courses of study; and
• Assessment of competence (following training).

Competence following training can be assessed by:

• Verbal or written tests;
• Self-evaluation;
• Observation of the individuals or teams;
• Assessment during continued coaching or mentoring;
• Participation in exercises designed to evaluate competence;
• Group coaching and challenges; and
• Recognition of professional qualifications.

Competence records may include:

• Staff training records – attendance at courses, seminars and conferences;
• Education and academic qualifications;
• Previous relevant experience;
• Competence or skills demonstrated during interview;
• Professional qualifications; and
• Staff appraisals.

The training programme may have to take into account:

• Changes to business processes that affect organizational priorities or operation;
• Legislation or regulation affecting the BCM programme;
• Change in perceived threats and vulnerabilities; and
• Corporate and client/partner requirements for the availability of information and services, including compliance with relevant standards.

Managing an Awareness Campaign

Prior to embarking on an awareness campaign it is important to establish the current level of awareness of BC. The objective should be to discover any gaps in awareness of, and commitment to, BC across the organization.

Sources of information could include:

• **Documentation**: including corporate policies and procedures, incident reports and accounts of previous BC exercises;

• **Feedback from staff**: including interviews with Top Management, management teams, and focus groups of staff from all levels;

• **Observation**: including on-the-job reviews of current working practices (for example, in comparison with corporate policy); and

• **Internal and external Audit reports** and any related non-conformities reported during a certification process.
Specifying the desired level of awareness is about the attitudes and behaviours that will meet the required level of awareness across the organization.

The specification will depend on the nature, scale and complexity of the business, and may include the following:

- Specific skills required for incident response;
- Enhanced working practices that improve organizational resilience by supporting the BCM programme;
- A better understanding of, and support for the BCM programme by staff generally; and
- A higher profile of BC in corporate decision-making, policy and culture.

Information resources for awareness campaigns may include:

- BC related websites, blogs and social media groups;
- Books, journals, periodicals and other industry publications;
- Conferences, workshops, webinars, and seminars;
- Regional forums and working groups; and
- Industry sector working groups.

The content of any staff communications aimed at raising the awareness of BC should be carefully considered and the appropriate channels used.

People are already likely to be the target of many awareness campaigns from other disciplines and may easily be overwhelmed by too much information. Co-ordination and co-operation with other departments is recommended. A joint Security, BC and Health & Safety briefing for staff may be more effective than separate events.

Communication should be brief and relevant but with the opportunity to find more information for those who are interested.

Suitable topics for such communications could be:

- A recent exercise – describing the scenario and learning points;
- A visit to alternative facilities – which might include a photograph and participant’s comments;
- Commentary on a recent incident which affected the organization; and
- Light-hearted real-life incidents with a BC related moral.

Outcomes and Review

The purpose of managing a successful awareness campaign is to increase knowledge levels across the organization. The benefits of this are that BC becomes part of the culture and the ‘way things are done around here’ and this increases the organizations ability to foresee threats, and respond appropriately in a timely manner and therefore improve levels of resilience.

Review and evaluation should address the desired level of awareness agreed at the outset.
BCI Professional Practices
PP3 - Analysis
Overview

Analysis is the Professional Practice within the BCM Lifecycle that reviews and assesses an organization in terms of what its objectives are, how it functions 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.

The main technique used for the analysis of an organization for Business Continuity (BC) purposes is the Business Impact Analysis (BIA).

However the BIA is not a one-time or single phase activity. Initially, it can help clarify the scope of the BCM programme, whereas it then becomes part of the ongoing activities to confirm business priorities and the resources required for continuity and recovery. At a strategic level, it can ask questions of Top Management which relate to the mission of the organization, its goals, targets, objectives and priorities. It can also be used at the tactical and operational levels to drill down and identify more detailed information.

Traditionally, analysis of the actual resources required for continuity and recovery has been considered a separate activity to the BIA, but in reality is almost always done as part of an operational level BIA. This guide has brought the analysis of resources within the overall BIA framework. This will cover the estimation of resources, facilities and external services that each activity will require at both resumption and return to normal operations.

A secondary method used in the analysis of an organization is known as “threat evaluation” which is used to estimate the likelihood and potential impact on specific activities from known threats. Threat evaluation is part of the wider methods used for risk assessment by organizations. Measures can then be identified to reduce the probability of occurrence or 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, 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. This is covered in the Design stage.

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

Business Impact Analysis

Introduction

The BIA is the foundation on which the BCM programme is built. It identifies, quantifies and qualifies the impacts in time of a loss, interruption or disruption of business activities on an organization and provides the data from which appropriate continuity strategies can be determined. 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.

General Principles

Different types of BIA are:

- **Initial BIA**: To develop a framework for further analysis and clarify the BCM programme scope;
- **Strategic BIA**: To identify and prioritize the most urgent products and services and determine the organization’s recovery timescales and disruption tolerance levels at a strategic level;
- **Tactical BIA**: To determine the process or processes required for the delivery of the organization’s most urgent products and services and assess the impact of a disruption on them at a tactical level;
- **Operational BIA**: To identify and prioritize the activities at an operational level which contribute to the identified process or processes that deliver the most urgent products and services, and to determine the resources required for the continuity and recovery of these activities.

A small or simple organization may be able to combine the tactical and operational BIAs. Alternatively an organization may decide its processes match its products closely enough that the strategic and tactical BIAs can be merged.
Concepts and Assumptions
The BIA looks at the products and services that an organization delivers and the activities and dependencies that underpin those deliveries. For each product or service, the purpose of a BIA is to:

• document the impacts over time that would result from loss or disruption;

• identify the maximum tolerable period of disruption or outage;

• determine the priorities for recovery; and

• identify the dependencies and resources (both internal and external) that are required to achieve agreed service levels.

ISO 22301 describes the above period of disruption as ‘the time within which the impacts of not resuming the activity would become unacceptable.’ The following two terms are commonly used to describe it:

• maximum acceptable outage (MAO), or

• maximum tolerable period of disruption (MTPD) which is defined as the time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.

For this GPG the term ‘maximum tolerable period of disruption’ (MTPD) is used.

Process
There is no ‘one size fits all’ methodology for BIA data collection. Methods vary from one industry sector to another, as well as from one BC professional to another. Each industry has its own specific needs for content, information types, depth and coverage.

When conducting a BIA the following should also be noted:

• At the start of the initial BIA there may not be a fully agreed scope. The assumptions about scope might need to be modified as a result of the initial BIA findings;

• Determining impacts over time will demonstrate to Top Management how quickly the organization needs to recover;

• There is a need to use a consistent BIA methodology and framework across the organization;

• The methodology used should be robust enough to ensure that data is collected consistently and impartially, thus ensuring that individuals do not over or under emphasize the urgency of their activities;

• Only pertinent and relevant data that can be used in the analysis should be collected;

• Impacts cannot normally be precisely determined; and

• When a BIA is undertaken for the first time in an organization an appropriate structure for analysis may not be clear, so this forms a significant part of the process. However once the initial BIA is complete, the organization can adopt a structured approach for subsequent reviews.
Methods and Techniques
The MTPD could be reached when, for example:

• Customers withdraw from their contracts and the organization cannot attract new ones;

• The reputation of the organization is so badly damaged, through a delivery, legal or regulatory failure, that interested parties no longer want to be associated with it;

• The organization is, or will soon be, bankrupt or in administration; and

• External pressure from interested parties forces a major change in the organization’s leadership or strategy.

The main factors that can be considered in estimating the MTPD of a disruption to product delivery or activities are:

• Damage to reputation or interested party confidence;

• Damage to financial value or viability (short- or long-term); and

• Failure to fulfil the objectives of the organization.

Delivery failures in different sectors can result in one or more of the following:

• Health implications from a service failure: for example, infections caused by uncollected household waste, which would also cause bad publicity and financial penalties;

• Breaches of statutory duties or regulatory requirements: for example, fines and reputational damage resulting from failure to settle share trades within the required time periods;

• Financial impacts: for example, loss of sales income, cash-flow problems caused by delayed payments and penalties from contractual breaches;

• Environmental damage: for example, leaks of chemicals due to delays to maintenance or the inability of a response organization to mobilise clean-up operations, resulting in bad publicity and financial penalties;

• Set-backs on major projects, research projects or a new product launch: for example, delay to a development project and loss of expected revenue; and

• Opportunities for competitors: for example, a government department failing to deliver a service and that function then being offered to a private company.

Seasonality and variability may affect the MTPD and therefore make it difficult to determine. In such instances, BIA should focus on an interruption to the activity during vulnerable periods of peak delivery, regulatory compliance or limited resource for the organization. Examples include:

• At financial year-end the MTPD for the finance activity is shorter than during the rest of the year;

• A one-off contract with significant time penalties may reduce the MTPD for a range of activities within the organization for the period of the contract; and

• The organization may experience peak demands and reduced MPTD times at, or approaching, holiday periods.

The duration or lead time of the process may be a significant factor in the MTPD estimate. For a process that takes a significant time, assumptions may have to be made in setting the MTPD, for example, at what point the disruption occurs and how much of the process needs to be repeated. For instance, a laboratory experiment may need to be restarted from scratch if interrupted, whereas a manufacturing process may be able to resume at several different points.

The MTPD can also be difficult to determine if the outcome of the disruption is uncertain, for example:

• The result of a delay in response at an emergency control centre will depend on whether any accidents occur during the time of the disruption; and

• A disruption to trading will inevitably be unpredictable as share prices can move in the opposite direction to those predicted during the interruption. The MTPD only needs to be accurate enough to establish the boundary or limits for the required recovery time. This is usually estimated as minutes, hours, days, weeks and months.
The recovery time objective (RTO) is the period of time following an incident within which a product or an activity must be resumed, or resources must be recovered. (SOURCE: ISO 22301:2012) It must be less than the MTPD by an amount which takes organizational risk appetite into account. Logically the RTO is determined in the Design stage of the BCM Lifecycle as it is a decision (not a finding) but an initial estimate can be made during the BIA which can be confirmed in the later stage once all the information is available.

The minimum business continuity objective (MBCO) is a minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption. (SOURCE: ISO 22301:2012) This level may be less than normal, the same as normal or at a higher level - perhaps to remove a backlog. The MBCO should be designed to be achieved at a specific time after a disruption. It may be appropriate to set several MBCOs for different times after an incident and for each product group.

Outcomes and Review

The words “critical” and “key” are often used to describe activities, products and personnel. These words are often understood in their common usage as “important” but this can lead to misunderstandings and exaggerations when collecting data for the BIA. It could result in an incorrect assumption that recovery tactics and plans are not required for “non-critical” activities or “non-key” personnel.

After ascertaining 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 (for example, one day, two day, one week, etc.); others use the term critical (or “mission critical”) for activities required within the first few days. It would be better to use terms with less ambiguous, time related meanings, such as “prioritized activities” (as used in ISO 22301:2012), “time sensitive” and “urgent”. Likewise for personnel the focus should be on staff whose absence would cause the quickest unacceptable impacts. This may be very different from their status (importance) in the organization’s hierarchy.

It is possible some information will be market/industry sensitive and so, in some organizations, it may not be visible to the BC professional. Not having this information should not stop the BIA being undertaken but could affect the accuracy of the end results and should be noted in the conclusions.
The Initial BIA

Introduction
When an organization embarks on its first BIA, it is often not clear how best to describe the organization in terms of products and services, processes and activities for analysis purposes. This is because organizations normally manage products and services by functional similarity and describe their operations by department.

General Principles
The initial BIA must develop an analysis framework for the business and may need to combine the tasks of strategic, tactical and operational BIA. The framework may also be used to clarify the BCM programme scope.

As a result of the exploratory nature of the initial BIA, the scope may have to be adjusted during the course of the exercise and the timetable for its completion may have to be flexible.

Concepts and Assumptions
This is in line with the concept of continual improvement as defined for a Business Continuity Management System (BCMS), a technique which continually enhances and refines the results of the BIA until it satisfies the organization’s scope.

The minimum objective of an initial BIA is to identify the product and services, and the processes and activities within the organizational structure. MTPD’s can be estimated with activity and resource analysis as time allows. From the perspective of being seen to make progress on the BCM programme, a timely delivery of the initial BIA may be more important than the detail as long as it is delivering business value to the organization.

It is necessary to obtain the full support of Top Management before attempting an initial BIA. Managers are unlikely to be prepared to dedicate time to this exercise without this backing.

There are a variety of proprietary software products available to conduct BIAs that may be useful but not essential. The key benefits of using a software tool include ease of collating results, storage of information and reporting the results. Their use does not remove the need for interviews with or involvement of individuals who are knowledgeable in the activity being analysed.

Process
The process includes:

1. Deciding the terms of reference and draft scope of the initial BIA;
2. Understanding the potential impact of significant future developments within the organization or the environment within which it operates;
3. For analysis purposes, assigning the products and services of the organization to groups based on urgency of delivery, splitting by customer and location if required;
4. Agreeing impacts to be considered as well as the criteria to determine the level of unacceptability;
5. Documenting impacts in time to the organization of a failure to deliver these product groups;
6. Estimating a MTPD for each product group and agreeing that with the project sponsor;
7. Identifying business processes across the organization that deliver the products (which may cut across several departments);
8. Identifying management owners for each process and suitable staff, such as subject matter experts, to provide information about the business processes;
9. Identifying how and when a disruption to the process could result in damage to the delivery of products and services;
10. Reviewing specific impacts which might not be fully appreciated by Top Management such as:
   a. Backlogs and capacity issues;
   b. The duration or lead time of the process;
   c. Any non-standard or unique activities which are difficult to recover and could unexpectedly delay the resumption of the process; and
   d. Presenting the findings to Top Management for review and approval.
A process is described as a set of interrelated or interacting activities which transforms inputs to outputs. (ISO 22301:2012). This input to output process may require effort from a variety of departments and is the level at which the tactical analysis will be undertaken. Examples of a process could be manufacturing (from goods receipt to delivery); investment management; or waste collection.

A process may be divided into a number of activities for an operational level analysis. An activity defined as a process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products and services. (ISO 22301:2012) For ease of data collection and subsequent development of activity recovery plans it is usual to define activities belonging to just one department in an organization. Examples are: perform quality control; undertake home care visits; raise invoices; and answer calls to a help desk. The level of detail to which activities are defined may depend on the complexity of their recovery and whether distinct MTPDs can be identified for each; otherwise similar activities can be grouped together.

Products and services are defined as “beneficial outcomes provided by an organization to its customers, recipients and interested parties.” (ISO 22301:2012).

**Methods and Techniques**

Methods, tools and techniques to carry out an initial BIA include:

- Workshops;
- Questionnaire(s) – paper and/or automated software; and
- Interviews

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; and
- 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 create consistency of recording and analysing information across multiple processes.

**Outcomes and Review**

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. This is because requirements for the final report format may affect the way the information is collected, collated, analysed and presented.

**The outcomes from an initial BIA are:**

- An organizational structure of product and services, processes and activities;
- A list of all processes and activities that contribute to the delivery of product and services;
- The MTPD and its justification for each product, process and activity. This will help determine the priorities of the continuity and recovery strategies;
- Main activity dependencies – internal and external; and
- A list of products, services and processes that have been excluded, along with the justification for such a decision.

This understanding of the structure of the organization will allow future BIAs to be conducted at different levels. These can then be embedded in the regular maintenance cycles of the organization which is a more efficient and effective validation of information than a repetition of the all-inclusive lengthy BIA described above. An initial BIA should not need to be completed more than once unless there is a substantial change to the organization or if several years have elapsed since the last BIA.
The Strategic BIA

Introduction
In a strategic BIA, the organization’s products and services are identified and prioritized and the organization’s recovery timescales or Maximum Tolerable Periods of Disruption (MPTD) and disruption tolerance levels or Minimum Business Continuity Objectives (MBCO) are determined.

General Principles
The strategic BIA may also be used to clarify or review the scope of the BCM programme in terms of products and services. Top Management should identify significant future plans for the organization which may affect the impacts to be evaluated in the BIA.

A BIA can be used to determine the impact of interruption in advance of significant organizational 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; and
• 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.

Process
The strategic BIA could follow the development or issuing of the organization’s strategic review (or a document which states the current business objectives).

The process could include:

• Reassessing the scope of the BCM programme, reviewing any exclusions and considering the inclusion of new products;
• Understanding the potential impact of significant recent or future developments within the organization or the environment within which it operates;
• For analysis purposes, assigning products and services to groups based on urgency of delivery, split by customer and location if required;
• Reviewing impacts to be considered as well as the criteria to determine the Minimum Business Continuity Objective, (MBCO);
• Documenting the impacts in time to the organization of a failure to deliver each product group;
• Estimating a MTPD for each product group;
• Gaining Top Management sign-off; and
• Proceeding to a tactical BIA.

Outcomes and Review
The outcomes of a strategic BIA include:

• A validation or modification of the scope of the BCM programme;
• Approved MBCO for the organization, signed off by Top Management;
• Approved MTPDs (and possibly draft RTOs) for each group of products and services; and
• A list of the organization’s most urgent groups of products and services.
The Tactical BIA

Introduction
A tactical BIA determines the process or processes required for the delivery of the organization’s most urgent products and services and assess the impact of a disruption on them.

Concepts and Assumptions
The scope of the tactical BIA may be a subset of the strategic BIA scope – examining the impacts of disruption to one or more product and service groups.

In some cases, such as a customer call centre, for the product and service, the process that delivers it and their recovery priorities may be the same. In others (often where the process takes time), it is useful for analysis to treat the final product and services as outcomes of processes that result from a combination of activities, supplies and contractors, all with different time priorities.

Process
This will include the following activity:

- Identify owners for processes;
- Approval of the terms of reference for the BIA with the owner of the process;
- Determine the scope of the tactical BIA:
  - The scope should be described by the product and service groups under examination as defined in the strategic BIA; (If it is estimated that 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);
- Identify the dependencies for the processes that deliver the most urgent products and services (which may cut across several departments);
- Identify suitable staff, such as subject matter experts, to seek information about the business processes;
- Identify how a disruption to the process could result in disruption to the delivery of products and services;
- Using the MTPD of the product group as a guide, quantify the timescale within which the interruption of each process would become unacceptable because of disruption to the delivery of products and services:
  - This may need to take into account impacts not factored in by Top Management, such as backlogs and capacity issues;
  - The duration or lead time of the process;
- Estimate Recovery Time Objectives (RTOs) for the processes;
- Estimate Recovery Point Objectives (RPOs) for the processes;
- Obtain approval by the process owner to confirm accuracy of information in the tactical BIA;
- Obtain the support from Top Management for the conclusions of the tactical BIA;
- Publish the results of the tactical BIA.
Methods and Techniques
The tactical BIA will build on the results of the strategic BIA. It provides guidance in identifying significant timeframes which can be used to tabulate the impacts for each process. The tactical BIA will also help verify the conclusions of the strategic BIA. A number of time periods for analysis purposes will usually need to be agreed, but how many and their exact values will differ between industry sectors. In some sectors, impacts may reach unacceptable levels within minutes, whereas in others an organization might not experience serious effects until there have been several days of disruption.

Outcomes and Review
The outcomes of the tactical BIA are:

- A list of processes that contribute to the delivery of the organization’s most urgent product and services within scope; and
- The MTPD (a draft RTO and possibly RPO) and its justification for each process.

The Operational BIA

Introduction
The operational BIA identifies and prioritizes the activities at an operational level which contribute to the identified process or processes that deliver the most urgent products and services, and determines the resources required for the continuity and recovery of these activities.

General Principles
The operational level BIA is where the detailed information about the resources required to continue, recover and resume activities to support the organization’s objectives and obligations, is collected.

Dependencies on external suppliers can be determined at this level when determining resource requirements. It is usually appropriate to identify the common ones such as utilities (power, water, telecoms etc.) also at the tactical level since they affect most processes.

Concepts and Assumptions
It is often assumed the resources required after a disruption will be a fraction of those 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 normal, to cope with backlogs. For example, in a call-centre, additional staff may be needed to cope with extra calls following an interruption and supporting information communication technology (IT) systems may need to have a higher capacity to cope with an additional number of users.

The loss of data can make it difficult for an organization to recover its operational capability. Some activities may be able to operate adequately with no data, or with data that is several weeks old. A few activities cannot tolerate any loss of data, although most can tolerate some loss.

ISO 22301:2012 describes the point to which information used by an activity must be restored to enable the activity to operate on resumption as a “recovery point objective” (RPO) which the standard also refers to as “maximum data loss”. The maximum data loss should be determined in this Analysis stage of the BCM Lifecycle.

The reason for collecting resource information at this stage is to:

- Provide the resource information from which an appropriate recovery strategy can be determined and recommended to Top Management; and
- Identify resource requirements resulting from activity dependencies that were identified at a tactical level that exist both internally and externally.

Process
The process for determining the most urgent activities at an operational level is similar to the process adopted for conducting a BIA at the tactical level. The focus, however, is on individual activities, which could be at a departmental or single business unit level rather than on processes determined at a tactical level (which could cut across many departments or business units depending on the nature, scale and complexity of the organization.)

The process should:

- Identify and prioritize the activities which contribute to the process or processes that deliver the most urgent products and services;
- Quantify the resources required in time to maintain the
Methods and Techniques
During the operational BIA it is necessary to collect information about the resources required to resume and continue the business activities, supporting the organization’s objectives and obligations.

Resource requirements can be collated with activity MTPDs to produce tables such as:

- Cumulative resource requirement by department and time;
- IT service requirements by time; and
- Dependencies that would impact the top level business process.

The operational BIA data collection should be undertaken by a suitably trained departmental representative.

Outcomes and Review
The outcome from an operational BIA is:

A list of internal and external resource requirements for the continuity and recovery of the organization’s most urgent products and services.

The operational BIA should be reviewed for those activities affected by organizational change. Other activities may require only a sample review and validation of the previous BIA results. This information feeds directly into the Design stage of the BCM Lifecycle.

Threat Analysis
Introduction
The process of evaluating threats uses risk assessment techniques to identify unacceptable concentrations of risk to activities and single points of failure, so measures can be considered in the Design stage that may lower the likelihood or decrease the impact of disruption to them.

General Principles
The BIA documents the impacts in a period of 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.

Concepts and Assumptions
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 industry 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 the BCM programme is not the same as undertaking a Risk Assessment. It is often undertaken at a lower level of detail. Using risk assessment techniques as part of BC may inform an existing Risk Management programme but that is not its primary purpose.

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).

Whilst reasonably effective at dealing with known and predictable threats, they have serious shortcomings in evaluating the threats posed by catastrophic operational situations 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 (for example, 1 for low, 2 for medium, 3 for high) over-emphasise the impact of minor events and cannot be used to calculate a comparative measure of risk for example, does a low probability and high impact risk have the same value as a high probability risk with low impact?; and
- 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 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 impact on the most urgent activities;
- Identify unacceptable areas of risk or single points of failure;
- Identify and record previously unknown or non-documented risks where no cohesive process exists for undertaking such activities during a disruptive incident; and
- If the organization has an existing Risk Management control programme, pass the results of the threat evaluation to the person responsible for the programme.
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, 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;
• Interested party 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; and
• Network analysis.

Probabilities can be assessed using:

• Insurance statistics; and
• Published disaster frequency statistics.

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; and
• The identification of any unacceptable single points of failure.

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; and
• There is a significant change in the external business environment – such as market, legal or regulatory change.
BCI Professional Practices
PP4 - Design
Overview
Design is the Professional Practice within the BCM Lifecycle that identifies and selects appropriate strategies and tactics to determine how continuity and recovery from disruption will be achieved. Information obtained from the Analysis stage and decisions made at the Policy and Programme Management stage are used to design solutions in the following three areas:

Continuity and recovery strategies and tactics; Threat mitigation measures; and Incident response structure.

Continuity and Recovery Strategies and Tactics

Introduction
The purpose of designing continuity and recovery strategies and tactics is to set timescales for recovery and identify the means by which those objectives will be best achieved. This can be undertaken at three organizational levels:

- Strategic – products and services;
- Tactical – process infrastructure; and
- Operational – activities that deliver the products and services.

At a strategic level the relative importance of various products and services has been determined in the Analysis stage.

At a tactical level, the process infrastructure consists of the services and facilities needed to deliver a product or service. It is where:

- The solutions which will make plans workable in practice are designed; and
- Decisions are made which will probably incur the most expenditure.

The design of operational solutions might require technical skills beyond those of a BC professional. Technical advice might need to be sought from experts in other fields, in particular for manufacturing businesses. Typically, specialists in Informational Technology (IT), Purchasing and Supply, Inventory Management and Capacity Planning might be needed to help determine the strategies and tactics that will be appropriate.

General Principles
The Analysis stage of the BCM Lifecycle identified the maximum tolerable period of disruption (MTPD) of the organization’s products and services, processes and activities. This Design stage finally sets the agreed period of time for the resumption of each of these, which is known as the recovery time objective (RTO).

The RTO for each product, service, process and activity should be set at less than its MTPD. Care should be exercised to ensure the aggregate RTO of processes, activities and dependent services do not exceed the MTPD of the overall process. This will ensure that individual interruption will not threaten the overall survival of the organization.

The Recovery Point Objective (RPO) is the point to which information used in an activity must be restored to enable the activity to operate on resumption (can also be referred to as “maximum data loss”) (ISO 22301:2012)

Concepts and Assumptions
Balancing cost and speed of recovery: If cost was not a consideration, it would be possible to define and implement a perfect solution. In practice there is always a trade-off between cost and the speed of recovery. In most situations, it is true that the shorter the RTO and RPO, the greater the cost to the organization, while the longer the RTO and the RPO, the cheaper the solution. Typically longer RTOs increase the chance that the recovery will not be achieved within the MTPD. Longer RPOs increase the chance that data will not be recovered.

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

Strategies:
There are a number of general strategies for continuity and recovery that can be deployed:

- Diversification;
• Replication;

• Standby;

• Post-incident acquisition;

• Do nothing; and

• Subcontracting.

In addition, Insurance is a strategy used to provide financial compensation for loss and disruption. Continuity strategies selected need to take into account the insurance cover that the organization has arranged.

**Tactics:**
The design of continuity and recovery requires tactics to be selected that can be deployed in the event of the loss of:

• People (skills and knowledge);

• Premises (buildings and facilities);

• Resources (IT, information, equipment, materials, etc.); and

• Suppliers (products and services supplied by third parties).

Although the tactics selected need to work in isolation (for example, if the only loss is of a computer system or single production line), they also need to work together in any combination (for example, when a building is lost in an incident that destroys all the resources in the building, renders some of the staff unavailable for work and also disrupts a local supplier).

Due to the vast differences in types of businesses that will implement BC it is not possible to be prescriptive in this GPG about what would be suitable for which organizations, sectors or geographies.

Tactics should also address how the short and longer term funding to employees and the organization will be provided.

**Methods and Techniques**

**Strategies:**

**Diversification:** The diversification of activities and resources to ensure continued operations requires the live undertaking of activities at two or more geographically dispersed places so that, in the event of the loss of one operation, the activity can continue at the other sites. 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:** Copying resources to enable operations to be recovered quickly is a variation on diversification in that the replicated site is dormant, being brought into live operation after an incident. Replication provides the capability to undertake all the activities required but will usually necessitate moving the required people to the replica location after the incident.

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 activities within their RTOs. However, the strategy relies on staff being both able and willing to work away from their normal location for what could be a prolonged period of time.

**Standby:** Where the RTO is greater than a day, an appropriate strategy may be to have a standby facility available that can be made operational within the RTO. This is particularly suitable where a facility has been temporarily shut down but is capable of becoming operational at short notice. It too relies on staff being both able and willing to work away from their normal site for what could be a prolonged period of time.

**Post incident acquisition:** Acquiring the resources required to undertake activities after an incident from a list of requirements is suitable for RTOs measured in days or weeks and depends upon having pre-qualified suppliers providing resources at short notice. This would not be an appropriate strategy where there is a requirement for specialist equipment, facilities or skills that might be difficult to obtain or which have long lead times.
It is important to note that typically BI insurance may cover loss of business revenues (gross margins) and/or additional costs of working, 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 political or commercial reasons, but this is generally prohibitively expensive for all but the largest of global corporations.

Insurance can also provide financial compensation following the loss of named key individuals due to death, injury or resignation.

It should be noted that an Insurance policy in itself does not provide for continuity of operations unless the organization's RTO's are measured in months or years because recovery efforts and co-ordination themselves can take many months to complete following any disruption.

**Tactics:**

**Safe separation distance:** To improve its continuity and recovery capability, an organization may keep duplicate copies of vital resources, use multiple suppliers, replicate operations in different locations or designate recovery sites. As many incidents frequently result in the loss of access to, or damage in a geographic area or location, there needs to be an adequate separation between the original and duplicate resources, the various suppliers, the replica operations or the base site and its designated recovery site. Consideration can be given to the use of organizational and government risk registers, which may provide useful information in terms of possible geographical threats and their relative potential impact.

The selection of a safe separation distance will determine the maximum geographic extent of an incident that the organization is able to directly recover from and this should have been selected as part of the process of developing a BC policy. That selection will depend on the organization's strategy, objectives and culture. Some organizations can use their market area or jurisdiction to define this, while others may choose the pragmatic alternative of placing a relocation site within the limit of how far they judge their staff would travel.

One way to determine the distances is to look at the threats identified in the Analysis stage and how they relate to specific geographic locations. For example, a secondary location with different power grids and providers to the
Design

primary site might be required for organizations (such as manufacturing) where loss of utility power is a major risk to continuity of operations.

Whilst greater geographical dispersion usually decreases the likelihood of two sites being affected by the same incident, for some threats, such as pandemics and global computer viruses, it does not necessarily provide protection.

Service levels: Many organizations will have identified only the minimum level of service that is acceptable to achieve its immediate business obligations during a disruption. This has been defined in the Analysis stage as the minimum business continuity objective (MBCO). Others will have identified a phased level of resources required to enable service levels to be increased through a period of time from the minimum acceptable level to a normal level.

Design detail: The extent and detail to which continuity, recovery strategies and tactics need to be designed will depend on the urgency with which they are required and the complexity of the process, infrastructure or activity being recovered.

A detailed design will be required for processes and activities with short RTOs, but recovery may not need to be designed in detail for those where the RTO is weeks or months, unless deemed necessary by the organization. In such cases, the organization may want to use the incident as an opportunity to change the way that it operates.

Reliability: When the continuity and recovery tactics considered involve third party provision of services, there is often a management decision to be made between the cost and the reliability of a 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.

The needs of interested parties: 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 businesses 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 clearly understood. The organization should ensure that the needs of various interested parties are identified, prioritised and agreed when designing the response, otherwise they may impede the subsequent recovery effort. For example, local residents could press the local authorities to refuse permission to rebuild on a damaged site.

Civil emergency responders: The organization should be familiar with the procedures of the local emergency responders and make contact with these groups in advance. This may provide useful information in assisting with the design of continuity strategies and tactics.

The availability of third party services: Third party alternative site arrangements are widely available in many countries and the options vary widely. However, in some countries the required services may not be commercially available and some governments will not permit organizations to source such services outside their country boundaries.

Where the third party recovery services required are not available, this will lead to the organization re-evaluating its design. One outcome may be that the organization decides to provide its own recovery facilities and possibly offer to share them commercially with other organizations faced with the same dilemma. This approach is particularly relevant in countries where third party providers have yet to establish a business presence.
Process
As with the analysis of BC requirements, the design of continuity and recovery strategies and tactics should be undertaken from top down at all levels within the organization. Once the design has been completed, the resources that are to be provided through the selected strategies and tactics need to be consolidated to deliver an organization wide view of the resource requirements.

Strategic: At the strategic level, RTOs for products and services are determined and strategies that will enable those RTOs to be achieved are selected.

The key steps in the process, which need to be undertaken for each product or service within the scope of the BCM programme, are:

- Identify the MTPD and deciding on the RTO (such that the RTO is less than the MTPD);
- If a phased level of resumption is required, identify RTOs for each service level;
- If there are any existing processes or procedures, conduct a “gap analysis” to identify where existing performance is measured against the required performance;
- Identify suitable strategies that will enable each RTO to be achieved;
- Analyse the strategic options for effectiveness and cost; and
- Provide Top Management with an evaluation of the strategic options, findings and a recommendation.

Agreement on the strategies to be used needs to be obtained from Top Management. This should include the expected capital and operational expenditure as well as resource provisions required to deliver the products or services to the agreed service levels.

Tactical and Operational: At these levels RTOs for any process infrastructure and activities required to deliver each product or service to the agreed service levels are determined, while the continuity and recovery tactics that will enable those RTOs to be achieved are selected. These tactics need to be selected in the context of the strategies that have been selected for the products and services and must ensure that the RTOs for the products and services are achieved.

It is not unusual to reiterate the selection of options to achieve an acceptable agreed balance between cost, effort and time to meet the strategic objectives of the programme.

The Analysis stage will have identified the processes and activities that are required to deliver the organization’s products and services, the activities that are most urgent and the resources required for the period to undertake the activities to agreed levels of service. Using the output from the operational BIA, the organization will know the process infrastructure and activities that need to be operational to deliver its products and services.

The key steps in the process, which need to be undertaken for the process infrastructure and activities required to deliver the product or service, are:

- Identifying the MTPD and deciding on the RTO (such that the RTO is less than the MTPD);
- If a phased level of recovery is required, identifying RTOs for each service level;
- If the process infrastructure or activities provide or use data, deciding on the RPO;
- If there are any existing response measures in place, conducting a gap analysis to identify where existing performance is measured against the required performance;
- Identifying suitable tactics that will enable each RTO and RPO to be achieved;
- Analysing the tactics for effectiveness and cost;
- Providing Top Management with an evaluation of the options and a recommendation; and
- Identifying implementation projects for each of the tactics selected.
Agreement on the tactics to be used needs to be obtained from Top Management, which should include the expected financial and resource provisions for their implementation.

**Consolidation:** The tactics selected for the process infrastructure and activities need to be consolidated by:

- Ensuring they are consistent across the organization;
- Verifying they do not conflict with one another (for example, that different activities are not planning to use the same resource for recovery);
- Verifying they do not infringe upon or contradict key organizational policies such as security of information;
- Determining how best to source external requirements (for example, third party recovery sites); and
- Assisting in designing the incident response structure and identifying the number of plans that may be required.

The key steps in the consolidation process are:

- Aggregate the recovery requirements from the tactics selected;
- Check that the selected options are consistent across the organization;
- Check that the selected options do not conflict with one another;
- Check that the consolidated third party recovery requirements can be obtained;
- Assess the resource implications of the selected tactics at the operational level;
- Re-evaluate the available options if found to be inconsistent or in conflict; and if necessary
- Re-confirm the high level strategic importance of the products and services;
- Provide Top Management with an evaluation of the consolidated requirements;
- Obtain agreement from Top Management to provide the financial and resource provisions for the implementation of the agreed measures; and
- Establish the projects for implementing the agreed measures.
Outcomes and Review
The main deliverables from designing continuity and recovery strategies and tactics are:

- A set of continuity and recovery strategies and tactics agreed by Top Management;
- A design for continuity and recovery that will be used in developing the plans;
- The establishment of projects with appropriate funding and resources for implementing the agreed strategies and tactics;
- A consolidated set of third party resource requirements to be used in purchasing resources; and
- Sufficient detail to enable an incident response structure to be designed.

A review of the design should be carried out:

- At least once a year following the review of the analysis of requirements;
- After any recovery capability has been tested; and
- On any significant change in:
  - Products or services;
  - Process infrastructure;
  - Activities;
  - Legislative requirements;
  - Regulatory requirements;
  - Customer requirements;
  - People and skills;
  - Premises;
  - Resources; and
  - Suppliers.
**Threat Mitigation Measures**

**Introduction**
The purpose of designing threat mitigation measures is to identify and select proactive measures that can be implemented to reduce the likelihood and/or impact of disruption to the organization’s most time critical and urgent activities.

**General Principles**
Threat mitigation measures are targeted at unacceptable concentrations of risk, single points of failure and the main threats to the organization’s most urgent activities, all of which were identified and prioritised in the Analysis stage of the BCM Lifecycle. They form an integral part of the overall objective of increasing organizational resilience.

**Concepts and Assumptions**
The evaluation of threat mitigation measures assumes that the benefits of the proposed measures can be estimated accurately. Estimating the benefits relies on knowing the likelihood of a threat being realised, which in many cases is guesswork or based on historic information.

**Process**

**Cost Benefit Analysis:** Cost benefit analysis can be used to determine whether or not a threat mitigation measure is worth implementing by comparing the cost of the measure with the likely benefit to be obtained. In undertaking a cost benefit analysis, the time frame in which the threat mitigation measure will be effective and the likelihood of the threat being realised in that period need to be determined.

For measures that reduce the likelihood, benefit is calculated by estimating the reduction in likelihood of the threat being realised after the mitigation measure has been put in place and multiplying it by the impact on the organization if the threat was realised, in terms of cost.

For measures that reduce the impact, benefit is calculated by estimating the reduction in impact of the threat to the organization, in terms of cost, after the mitigation measure has been put in place and multiplying it by the likelihood of the threat being realised.
**Threat reduction:** Examples of specific threat reduction techniques and measures that can be adopted include:

- Physical security – to prevent theft and unauthorised entry;
- Information security – to prevent the loss of data and unauthorised access;
- Monitoring systems – to provide prompt warning of fire, utility failures, equipment failures and disruptive threats;
- Sprinkler and fire suppression systems – to prevent fire spreading; and
- Resilient telecommunications networks – to ensure there are no single points of failure.

Advice on physical security can be obtained from the various national and international professional security associations, many of whom publish guidelines and good practice.

Advice on information security is available from the various national and international IT and information security bodies.

The key steps in designing threat mitigation measures are:

- Review the output from the operational BIA and threat analysis to confirm unacceptable areas of risk, single points of failure and prioritised threats to the organization’s most urgent activities;
- Identify any measures that can be taken to reduce the likelihood and/or impact of disruption to the organization’s most urgent activities – threat mitigation measures;
- Analyse the threat mitigation measures for effectiveness and cost;
- Provide Top Management with an evaluation of the threat mitigation measures;
- Identify implementation projects for each of the threat mitigation measures selected;
- Obtain agreement from Top Management to provide the financial and resource provisions for the implementation of the threat mitigation measures; and
- Establish the projects for implementing the agreed threat mitigation measures.

**Outcomes and Review**

The main deliverables from designing threat mitigation measures are projects for implementing agreed mitigation measures to reduce the likelihood and/or impact of disruption to the organization’s most urgent activities.

The need for threat mitigation measures to be identified and selected should be re-evaluated:

- Annually;
- When there has been any change to the organization’s most urgent activities or the level of threat to their disruption; and
- When there has been an actual incident experienced by the organization, within a similar industrial sector or at a nearby location.
Incident Response Structure

Introduction
The purpose of designing an incident response structure is to ensure that there is a documented and fully understood mechanism for responding to an incident that has the potential to cause disruption to the organization, regardless of its cause.

General Principles
• An incident response structure identifies:
  • The teams responsible for response and recovery activity;
  • The relationships between the teams; and
  • The roles and responsibilities of the teams.

An essential feature in any response model is a mechanism to escalate information upwards and communicate decisions downwards.

The objective is for BC to become just a normal part of the way that the organization operates, so that unless there are valid reasons against it, the incident response structure should mirror the organization’s existing management structure.

There is no correct design for an incident response structure. Each organization should develop a structure that meets its own needs.

Concepts and Assumptions
The strategic, tactical, and operational levels in the response structure perform different roles:
Strategic – describes how Top Management will address and manage the issues resulting from a major incident;
Tactical – details the management and co-ordination of the recovery of operations that have been disrupted, ensuring that resources are appropriately allocated; and
Operational – addresses the recovery of activities or systems to pre-defined levels of service.

Methods and Techniques
Designing the Structure: The incident response structure needs to identify teams to cover emergency response, incident management and recovery. It also needs to identify which teams will undertake the strategic, tactical and operational roles.

In designing a structure, the following factors should be taken into account:
• The existing management structure;
• The organization’s nature, scale, complexity and process infrastructure;
• The continuity and recovery strategies and tactics selected; and
• The nature, scale, complexity and urgency of the recovery requirements.

In many organizations, emergency response plans will have been developed and implemented before the introduction of BC. In these cases, the people and teams responsible for using the emergency response plans should be incorporated into the incident response structure.

Similarly, many organizations will have developed and implemented strategic level incident management plans (often known as crisis management plans) before the introduction of BC. Again, the people and teams responsible for using these should be incorporated into the incident response structure.
**Roles and Responsibilities:** The roles and responsibilities of the teams identified in the incident response structure need to be identified and documented. These will include responsibilities for:

- Mobilizing teams;
- Activating plans;
- Invoking resources;
- Communicating to interested parties;
- Communicating to media;
- Staff welfare;
- Escalation;
- Command and control;
- Expenditure and delegation limits; and
- Changing priorities as the situation evolves.

**Process**
The key steps in designing the incident response structure are:

- Identifying the organization’s existing management structure, nature, scale, complexity, process infrastructure and activity recovery requirements;
- Identifying the people and teams responsible for using any existing emergency response, crisis management or incident management plans;
- Developing a draft incident response structure;
- Reviewing the draft incident response structure;
- Preparing a recommended incident response structure for Top Management;
- Obtaining Top Management approval for the incident response structure; and
- Documenting and publishing the approved incident response structure.

**Outcomes and Review**
The outcome from designing the incident response structure is a design that is used for developing and implementing the response, containing details of the:

- Response and recovery teams;
- The relationships between the teams; and
- The roles and responsibilities of the teams.

The incident response structure should be reviewed when there has been any significant change to the organization’s:

- BCM programme scope;
- Nature, scale and complexity;
- Management structure;
- Process infrastructure;
- Continuity and recovery strategies and tactics; and Specific activity recovery requirements; or
- If there has been an actual incident affecting the organization.
Design
BCI Professional Practices
PP5 - Implementation
Overview

Implementation is the Professional Practice within the BCM Lifecycle that executes the agreed strategies and tactics through the process of developing the Business Continuity Plan (BCP). The aim is to identify and document the priorities, procedures, responsibilities and resources to assist the organization in managing a disruptive incident, while implementing continuity and recovery strategies to a pre-determined level of service.

The key requirements for an effective response by the organization are:

• The ability to recognise and assess existing and potential threats when they occur and to determine an appropriate response;

• A clear and understood procedure for the activation, escalation and control of the organization’s incident response procedures (the incident response structure);

• Having responsible personnel with the authority and capability to implement the agreed continuity strategies (or objectives) as defined within the organization’s plans to continue and recover the disrupted activities;

• An ability to communicate effectively with internal and external interested parties; and

• Access to sufficient resources to support the BC strategy.

The outcomes can be achieved by various methods and techniques and, whatever approach is adopted, it is important that it is suitable for the needs of the organization.

The actions outlined in plans are not intended to cover every eventuality 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 created.

A variety of software products are available to assist in building and maintaining a BCP but these are not essential. Using everyday office software will often suffice and is more inclusive of all staff since its use does not require special training. Specialist software can provide benefits in the areas of plan management for large organizations.

The Business Continuity Plan

Introduction

Although the term “Business Continuity Plan” (BCP) implies a single document, it can exist at any organizational level and can accommodate any level of procedural detail. It can cover a complete organization or part of an organization and can be structured by products, services, locations, divisions or departments and, in certain extreme circumstances, for particular scenarios.

General Principles

The term ‘business continuity plan’ is defined in ISO 22301:2012 as “Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.”

Other terms may be used to describe this set of documented procedures, most typically emergency response plans and crisis management plans. Within these Good Practice Guidelines (GPG), these are simply considered as specialist forms of the BCP. Although clearly within the generic definition above, such plans might be managed separately from the BCP in some organizations and might need specialist expertise such as would be the case with plans to deal with kidnapping and extortion incidents for example.

In many organizations, Information Technology (IT) departments may refer to their plans as disaster recovery plans.

Other names for specialist plans which have the overall characteristics of a BCP include:

• Incident or Crisis Management plan;

• Contingency plan;

• Media response plan;

• Pandemic plan;

• Product recall plan;

• Major hazards plan;

• Disaster recovery plan;

• Service continuity plan; and

• Continuity of operations plan
In the context of this GPG, all these types of plan (however named) are considered part of the BCP.

**Concepts and Assumptions**

The BCP is intended to be used in high pressure situations when people are under stress. Plan design must take this into account, to make the document focused, specific and easy to use. Important characteristics for an effective BCP include:

- **Direct** – plans should provide clear, action orientated and time-based direction, while allowing quick access to pertinent support information;

- **Adaptable** – plans should enable the organization to respond to a wide range of disruptive incidents, including those that the organization may not have anticipated;

- **Concise** – plans should only contain guidance, information and tools that are likely to be used by the team in a disruptive incident. Anything else is superfluous; and

- **Relevant** – the information in the plan should be current and applicable to the team that will use it.

The BCP can cover any or all stages of the response to an incident from the initial response through to resumption of normal activities.

The BCP also needs to address the strategic, tactical, and operational levels at which every organization works. As there is no single, agreed definition as to what constitutes strategic, tactical and operational, the number and types of plan are determined by context rather than by theory.
There is no single solution for how to structure plans; a combination of general business experience, knowledge of the organization and BC expertise are required to find the most suitable structure for an individual organization. Feedback from various plan users and analysis of testing results can also assist in further improving the structure of plans as part of the maintenance process, described in PP6 the Validation stage.

Methods and Techniques

The strategic, tactical and operational 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 of the organization’s response.

- **Medium sized organization** - In a medium sized organization, the levels of response might be implemented as:
  - **Strategic** - an incident management plan, with a response team made up of the Top Management;
  - **Tactical** - a single plan covering the recovery of all the organization’s operations, with a response team consisting of the functional leaders or heads of departments; and
  - **Operational** - usually covered by the tactical plan, except for IT which, because of the technical detail required, has its own disaster recovery plan with a technical IT recovery team.

- **Large organization** - In a large organization, the levels of response might be implemented as:
  - **Strategic** - an incident management plan, with a response team made up of the Top Management;
  - **Tactical** - a number of plans, each one covering a major division, product, service or location, each with its own response team consisting of either the functional leaders or division, product or service heads responsible for the areas covered by the BCP; and
  - **Operational** - usually covered by the individual tactical plans, except for the main support functions of IT, Finance, Sites & Facilities and Human Resources (HR), each of which has its own specialist recovery or response team.

- **Large multinational organization** - In a large multinational organization, the levels of response might be implemented as:
  - **Strategic** - a global incident management plan, with a response team made up of the Top Management with global responsibilities, and an incident management plan for each territory, with a response team consisting of the Top Management from the territory. Multinational organizations often also have another level of strategic plan focused on regions;
  - **Tactical** - each territory could have a number of plans, each covering a major division, product or service, each with its own response team consisting of the functional leaders or division, product or service heads responsible for the areas covered by the BCP; and
  - **Operational** - each department or location covered by the BCP may have its own detailed operational plan, with its own recovery team made up of the operational managers of the department or location.

The incident response structure from the Design stage is used in determining the number and type of plans that make up the BCP. In general, there will be a one-to-one correspondence between the recovery and response teams and the plans they use.

Whatever form the response structure takes, a recovery or response team with clear procedures for responding to a disruptive incident needs to be established for each plan that is developed and implemented under the structure.

A **Strategic level plan** is a high-level plan that defines how strategic issues resulting from a major incident should be addressed and managed by Top Management. It has some special characteristics which differentiate it from
the tactical and operational plans which form the bulk of the plans.

The media response to any incident is usually managed at Top Management level. The Incident Management Plan may also be used when the incident falls outside the scope of the BCM programme. This might include incidents that do not result in operational disruption, such as a fraud or negative media exposure, and those where the impact is across a wider area than allowed for in the BC strategy, such as a national emergency.

**Tactical level plans** co-ordinate and manage the recovery of a defined part of an organization, ensuring 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. They 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 BC strategies.

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 remains focused and is co-ordinated. The tactical level plans may change the agreed priorities and recovery strategies to take into account seasonal changes, current business priorities, or if directed by Top Management.

If the event and subsequent disruption falls outside the scope upon which a tactical level plan was based, then the situation should be escalated to Top Management.

**Operational level plans** provide for the recovery of the business activities covered by the BCP from the beginning of the incident through the recovery phases. They are based upon the agreed recovery requirements and measures, providing procedures and processes for recovering activities to agreed levels of service.

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 HR, that may have a specialist role in supporting the overall recovery or provide specialist advice.
The recovery and response teams at the strategic, tactical and operational levels may not necessarily invoke their plans simultaneously. Activation may start at the operational level and escalate to the strategic level. Alternatively, activation 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 essential that the stand down process is controlled at all levels leading to a formal declaration that the incident has ended.

Developing and Managing Plans

Introduction

The number and type of plans to be put in place will have been determined using the incident response structure, the BC strategy and tactical options selected, the existing management structure and the nature, scale and complexity of the organization.

General Principles

Although the basic principles and approach to producing the BCP is similar in all situations, different degrees of emphasis are needed for different levels of plans. The need to involve Top Management in the development and implementation of plans is essential to achieve a successful outcome. Case studies of major incidents suggest effective and rapid management of an incident is the most significant factor in protecting an organization from operational, financial and reputational damage.

Concepts and Assumptions

Because the tactical and operational plans will contain information about recovery, they cannot be developed until the BC strategy and tactical options have been determined and agreed. In contrast, the strategic level plan does not usually contain such information and can be put in place at the start of the BC process to provide limited protection before the other plans are developed.

Each plan should always contain assumptions about the maximum scale of the incident that it has been designed to address, in terms of extent, duration or impact.

Process

The key steps in developing a plan include:

- Appoint an owner/sponsor for the plan;
- Define the objectives and scope;
- Develop and approve a plan development process and programme;
- Create a planning team;
- Agree the responsibilities of the response team and their relationship with other plans and response teams (strategic, tactical and operational);
- Create a response team having the required skills;
- Decide the structure, format, components and content of the plan;
- Determine the strategies, such as alternative locations, on which the plan will be 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 rehearsing it in an exercise; and
- Agree a programme of ongoing exercising and maintenance of the plan to ensure it remains current and response teams are up to date.
Implementation

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

- Meetings and interviews (structured and unstructured);
- Checklist(s); and
- Workshops.

Plans must be concise and easy to read. They are intended to be used in high pressure situations when people are under stress. Plans are not reports and should not include unnecessary information that will not be needed during a disruptive incident.

Plans 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 in the organization maintains an overall “master” version that contains all sections of the plan.

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

It is essential that all plans are held in publicised (and where necessary secure) locations for key interested parties requiring access. Where plans are held electronically, care should be taken to ensure these will be accessible during periods of disruption should, for example, the organization’s document management system become unavailable.

Where prudent to do so, hard copies should be taken of the plans and stored in known locations. This should also include copies of any additional material or ‘links’ referenced within such plans.

All plans at all levels should contain a number of similar elements:

- Purpose and scope;
- Objectives and assumptions;
- Incident management structure (for the organization as a whole);
- Response team responsibilities;
- Response team membership (leader, primary members and deputies);
- Individual responsibilities of the team members;
- Team mobilisation (instructions);
- Plan Activation (procedures and authorisation);
- Invocation (of recovery arrangements);
- Contact details (usually held as appendices);
- Team meeting room (command centre) locations;
- Communications (covering employees, contractors, interested parties, customers and the media);
- Key information from previous stages of the BCM lifecycle, such as details of the organization’s prioritised activities and timeframes;
- Action lists; and
- Procedures for standing down the team and organization once the disruptive incident has been resolved.

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

**Roles and Responsibilities:**
The personnel nominated to be members of the team must have the necessary authority and capabilities to respond to an incident at the appropriate level (strategic, tactical or operational). The responsibilities of the team and roles of specific individuals within the team should be documented with this in mind. Deputies should be identified for each role.

Specific team roles, each with nominated responsibilities, may include:

- Team leader – who should ensure that the response team is activated, briefed and properly staffed. They can nominate or co-opt team members if necessary;
• People and welfare;

• Internal communications – to establish and maintain contact with other response teams;

• External communications – to establish and maintain contact with interested parties and the media;

• Operations;

• Technical support; and

• Administrative support, including a record keeper – to maintain a log throughout the incident.

**Team Mobilization:**
The plan should document the conditions or circumstances in which the team will be mobilized. The plan may include disruption levels or impact thresholds that can support incident assessment and enable timely decision-making and escalation by the team.

The plan should clearly state which members have authority to mobilise the team, the organization’s continuity objectives and the required support equipment or facilities. However, these procedures should be flexible and adaptable for the absence of one or more team members. It is better for the team to take action where there is doubt since it is easier to stand a team down rather than mobilise them after the incident has developed beyond their capability to effectively respond.

The means by which the team will be notified, mobilised and stood down should be documented so that it can occur in the shortest possible time. Many organizations now use automated notification systems for contacting staff following an incident.

**Meeting Room:**
The team should agree, in advance, a number of possible meeting locations favouring those with the required resources. The first notified should identify the most suitable meeting place and an alternative, based on the current situation information. Depending on the nature of the incident, the team may meet continuously or at set periods throughout the day.

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 location that provides secure, 24-hour access, such as a hotel, may be able to provide the required meeting room facilities.

For large-scale disruptive events 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.

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

- Communication – incoming and outgoing;
- Recording events, decisions, actions and issues;
- Monitoring information about the incident; and
- Controlled entry.

The following meeting room resources could be considered:

- Continuously available, stable power supply;
- A number of landline telephones, teleconference equipment and voice recording facilities;
- A computer and printer;
- Cell phones and mobile communicators with chargers;
- Secure access to e-mail, internet and fax;
- Log sheets;
- Printed copies of relevant plans and urgently required information;
- TV and radio equipment;
- Stationery;
- Whiteboard/flip charts and pens that work for recording incident details along with actions taken and decisions made by the team; and
- Access to:
  - Refreshments;
  - Transport;
  - Sleeping facilities on-site or nearby;
  - Toilet and washing facilities.

Necessary equipment and resources should be stored in a “battle-box” or “recovery box” that is kept in, or near to the command centre or in a secure accessible off-site location.

**People Activities:**

Organizations have a responsibility (which may be legally enforced) to safeguard the health, safety and welfare of their employees, contractors, visitors and customers. The BC strategy should take into account personnel and welfare issues during all stages of a disruptive incident. The organization’s personnel are more likely to co-operate willingly with the extra demands placed on them in a disruptive incident if their welfare needs are met.

Issues to consider include:

- Special needs including:
  - Family responsibilities;
  - Pregnancy;
  - Disability; and
- Dealing with issues relating to casualties 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 the organization's personnel and visitors;
• Communicating with staff and others on the site;
• Contact with emergency contacts;
• Contact next of kin;
• Transport assistance;
• Setting up a staff help line; and
• Translation services.

Subsequently there may be additional needs including:

• Counselling and rehabilitation services – this could be provided as part of an employee health package;
• Liaison with specialist services when dealing with next of kin;
• Temporary accommodation;
• Access to emergency cash or facilities;
• Welfare needs at alternative locations:
  • Special needs;
  • Refreshments;
  • Personal safety and security;
  • Transport and accessibility;
  • Appropriate training on replacement equipment; and
  • Toilet and washing facilities.

Emergency Services Liaison:
If the organization is responsible for its own site or premises, staff with an appropriate level of experience and authority should be appointed to liaise with the emergency services from arrival on site and subsequently as required.

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

While on the site, the emergency services instructions take precedence over those given by the organization's own management and staff.

Once emergency services have formally relinquished control and departed from the site, the organization will resume responsibility for its own site.

Communication needs to be undertaken with the following:

• Employees and contractors;
• Other parts of the organization;
• Relatives, friends and emergency contacts;
• Customers and clients;
• Shareholders, investors, board members or owners;
• Suppliers and service providers;
• Regulatory authorities;
• Members or sections of the public; and
• Media – local and national newspapers, radio, TV, internet, social and other media.

Responsibilities for communicating with each of these groups should be defined by the team as an integral part of the development of the incident response structure.

There is a practical consideration to ensure that communication messaging is prompt and effective. Emergency notification systems are often used by large organizations to cope with the sheer volume of calls required.
For smaller organizations there might be no cost justification for installation of automated calling systems, so manual means need to be identified and tested. The most traditional approach is the use of call trees and call cascades.

**Media liaison:**
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 the organization’s personnel on what they must do when approached by the media.

Plans should also contain information on what actions the organization’s personnel must take if they are involved in an incident which has, or is likely to attract media attention and who should they inform in the organization if contacted by the media.

**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. A maintenance programme should be put in place for each plan to ensure that it is kept up to date.

**Strategic Plans**

**Introduction**
Strategic plans define how strategic issues resulting from a major incident should be addressed and managed by Top Management.

Some incidents will require a strategic level response that does not result from physical disruption to activities (for example, those involving threats to reputation alone) and may therefore not involve a plan activation. However, it may result in a team mobilization for those who have roles and responsibilities for managing the area affected and potential reputational damage. In these situations it is almost always necessary to involve the strategic level team if only to make them aware of the situation in case it escalates.

It is important that an organization chooses a plan name that fits its own culture and structure. The use of existing, familiar terms for plan and team names can encourage understanding and acceptance.

**General Principles**
As, by their nature, all incidents are different, a strategic level plan is a set of high level information and guidelines that will be useful to the team tasked with activating a response to a disruptive incident.

Once activated, the strategic level plan should address the need to communicate with, and control activity between, all the involved interested parties. The content of a strategic level plan should be suited to the nature, scale and complexity of the organization.

The strategic plan may contain reference material on the strategies of different parts of the organization or generic response information for specific disruptive incidents, such as loss of building or major loss of IT. The aim is not to encourage micro-management of the incident but to provide the team with summary information, such as how the response will take place or the timescales involved.

**Concepts and Assumptions**
During a disruptive incident, the strategic level team members are accountable for the organization’s stability, continuity and reputation. They have the responsibility to implement and adapt the overall response strategy when the organization is threatened. Specific responsibilities of the strategic level team include:

- Establishing the strategic objectives of the response to the incident;
- Devising short-, medium- and long-term strategies, depending on the nature of the disruptive incident;
- Managing communications with all the involved interested parties, including the media;
- Approving external statements before they are issued and monitoring and adjusting as necessary the communications strategy;
- Monitoring the overall response and progress of recovery;
- Resolving conflicts in the response and recovery;
- Ensuring the response and recovery is in line with the long term interests of the organization;
- Identifying and maximising opportunities or advantages
arising from the incident;

- Approving significant expenditure;
- Ensuring the financial health of the organization; and
- Ensuring any response and recovery meets the organization’s legal and regulatory obligations.

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; and
- Facilities for monitoring and broadcasting on social media.

These are subject to budgetary constraints and service availability.

Communications

The communications plan should address how the organization will manage communication with internal and external interested parties, including the media. The plan may be included within the strategic level plan or it may exist as a separate document.

The communications plan should:

- Identify the internal and external interested parties/audiences, record their contact details and, where possible, define each group’s communication requirements or expectations;
- Define the available methods/channels for communicating with each interested party group, for example, internet, social media, local radio and national newspapers;
- Include a selection of communications methods/channels, so that the team is assured of availability even if the disruptive incident impacts one or more channel;
- Identify the group or person in the organization who has the responsibility, authority and technical knowledge to deliver communication via each of the available methods/channels. Where possible established relationships should be used to communicate with interested parties;
- Decide in advance who the organization’s public/media spokesperson(s) will be and then ensure that:

- The spokesperson(s) have been trained in their role;
- The process to create and issue media statements is known, including how they will be approved internally prior to release;
- There are sufficient people to brief the media at a central location as well as representatives who can be on site at a local incident;
- There is a designated technical spokesperson if appropriate to the incident; and
- Assign responsibility to monitor and review the interested party response to issued communications via each of the available methods/channels to assess its effectiveness and adjust messages as required.

If appropriate, the organization can work with specialists such as public relations companies to develop the media response and consider retaining an advisor for use during an incident. If possible, the organization should develop a relationship with key media people in advance of any incident. The organization may also consider the use of a media monitoring/cuttings service and the monitoring of social network sites and chat rooms.

The volume, variety and urgency for communications after a disruptive incident can be significant. The communications plan can accelerate the response if it includes pre-formatted messages or pre-written statements. The communications plan can:

- Anticipate much of the likely information that will be required by known interested parties, for example, employees, customers, and shareholders;
- Develop pre-written statements for these foreseeable communications, retaining the capacity for the message to be adapted to the timing and circumstance of the incident;
disruptive incident;

• Develop questions and answers for the most likely incidents; and

• Develop a set text on the organization which can go out to describe the company in public/media statements.

Outcomes and Review
The outcomes of the strategic planning process include:

• A plan that can support the organization’s Top Management during a disruptive incident;

• A plan for managing interested party and media communications during a disruptive incident;

• Evidence of incident management preparedness for internal and external interested parties; and

• Compliance with legal, regulatory and governance requirements.

A review or audit should be aligned with the review of other plans, strategies and tactics. The plan may also be triggered by significant business or organizational change or by significant change in the external operating environment.

Tactical Plans
Introduction
Tactical level plans pull together the response of the whole organization to a disruptive incident by facilitating the continuity and resumption of business activities. Those using the plans should be able to analyse information from the response teams concerning the impact of the incident, select and deploy appropriate strategies or methods from those available in the plans, direct the resumption of business units according to agreed priorities and pass progress information to the strategic level team.

General Principles
The content of such plans will vary from organization to organization. They will have a different level of detail based on the culture of the organization, the technical complexity of the solutions and the degree to which the response solutions differ from usual business operations. It is rarely possible to write an effective plan unless the key elements of the resumption strategy are in place or are well advanced in their planning.

Concepts and Assumptions
The plan should be action orientated and easy to reference under stressful conditions. It should not be prescriptive or include information or documents that will not be required during an incident.

It should 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 team.
**Process**
Specific steps in developing tactical plans may include the following actions:

- Appoint a person to manage the development of all the plans;
- Develop a planning process and schedule. Normally, beginning with the plans for the highest priority business activities where this is technically possible;
- Decide the structure, format, components and content of the plans; and
- Develop an outline or template plan to encourage standardisation of documentation but allow individual variations where this is appropriate and technically possible.

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

A tactical plan should include detailed procedures for the team to:

- Promptly respond to activation;
- Assess information and make decisions (Go/No Go);
- Mobilise the teams and invoke resources;
- Initiate response procedures and recovery activities;
- Communicate and receive information from other teams; and
- Monitor progress and report status to the strategic level team.

**Methods and Techniques**
Specific responsibilities of response teams may include:

- Co-ordinating and monitoring the response and recovery of subordinate teams;
- Allocating available resources to subordinate teams;
- Changing the agreed priorities and recovery actions to take into account seasonal changes, business conditions or on direction from the strategic level;
- Monitoring the main support functions of IT, HR, Sites and Facilities and Finance;
- Requesting or receiving information from other response teams;
- Reporting to the incident management team; and
- Mobilising specialist service providers as required, such as salvage and recovery suppliers.

Available resources might include lists of:

- Personnel;
- Welfare requirements;
- Alternative locations;
- Security arrangements;
- Technology, communications and data;
- Transportation and logistics;
- Other service providers and suppliers;
- Contact information to access those resources; and
- Resource requirements for resumption of each activity.

The plan might include:

- Organization contact information;
- Key interested party information and contact details (customers, clients, service providers);
- Secure location of legal documents – such as contracts, service level agreements and insurance policies;
- Contracted recovery workspaces; and
- Procedures for obtaining emergency cash.
Outcomes and Review

The review of the planning process includes:

- Approval by Top Management; and
- A framework within which the operational level plans can work.

Some information that can become out of date quickly, such as contact details, should be reviewed regularly, in line with BC policy. Other information should be formally reviewed at pre-defined intervals and validated through exercising.

Other triggers leading to a review are:

- A significant organization change (for example, acquisition, divestment, merger);
- A major business process change;
- A significant change in personnel; and
- A significant change in IT services.
Operational Plans

Introduction
Operational level plans cover the response by individual departments or business units to the incident. Lower 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 captured in one or more discrete plans that become the responsibility of the business unit to which they relate.

General Principles
Examples of operational level plans are:

- A business department plan to resume its functions within a predefined timescale;
- A HR response to welfare issues during an incident;
- Procedures to assist a tactical level team, often led by a department that deals with the physical incident response, salvage and restoration; and
- An IT department’s response to the loss and subsequent resumption of IT applications and services to the business.

Concepts and Assumptions
The complexity and urgency of the business processes may determine whether one operational plan covers a single activity or a department level plan covering several activities. Likewise these 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.

Process
The plan should be action orientated and easy to reference under stressful conditions. It should not include information or documents that will not be required during an incident.

Specific stages of the plan development:

- Appointing a person to manage the development of all the operational plans;
- Appointing a representative within each business unit to develop their plan;
- Developing a planning process and scheduled programme. Where technically feasible, begin with the plans for the most urgent business activities;
- Deciding the structure, format, components and content of the plans;
- Developing a modular, outline or template plan to encourage standardisation of documentation but allow individual variations where this is appropriate and technically possible;
- Documenting connections with the tactical level plans and between operational plans;
- Ensuring business units nominate individuals to fulfil key roles within their plans;
- Managing and co-ordinating the development of plans within the business units;
- Circulating the draft of the plan for consultation, reviewing and challenging within and, where necessary outside, the business unit;
- Gathering feedback from consultation;
- Amending the plan as appropriate; and
- Validating the plan through an exercise with the business unit.
Methods and Techniques

Plans may include instructions regarding:

- Staff welfare;
- Access to and use of facilities;
- Resumption of business unit activities within agreed recovery time objective levels;
- Liaison with IT service continuity teams; and
- Mobilization of teams and invocation of resources required for recovery purposes.

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

- Building evacuation and invacuation (for example, safe shelter) plans;
- Evacuation points (including alternate or off-site);
- Emergency services liaison;
- Bomb threat procedure;
- Redeployment of staff and visitors;
- Salvage resources and contracted assistance;
- Escalation procedures;
- HR and welfare issues;
- Health and safety liabilities;
- Procedures for accounting for staff;
- Procedures for contacting staff;
- Counselling and rehabilitation resources;
- Initial response on activation;
- Contacting team members;
- Resumption plan for each activity;
- Personnel contact numbers;
- Other key contacts;
- Procedure for resumption of business activity by time period and data requirements;
- Activity priorities by time period;
- Space, seating and resource requirements by time period;
- Special, or non-standard procedures;
- Work in progress issues; and
- Resources and materials required.

Outcomes and Review

The outcomes of the operational planning process include:

- Documented plans for departments or business units;
- Success criteria and stand down procedures; and
- Clearly defined 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 associated or related plans.
BCI Professional Practices
PP6 - Validation
Overview
Validation is the Professional Practice within the BCM Lifecycle that confirms that the BCM Programme meets the objectives set in the BC Policy and that the organization’s BCP is fit for purpose.

The purpose of Validation is to ensure that the BC capability reflects the nature, scale and complexity of the organization it supports and that it is current, accurate, and complete, and that actions are taken to continually improve organizational resilience.

Validation is achieved through by the following three activities:
• Exercising;
• Maintenance; and
• Review.

Developing An Exercise Programme
Introduction
A planned Exercise Programme is required to ensure that all aspects of the response to an incident have been exercised. In particular:
• All information in plans is verified;
• All plans are rehearsed; and
• All relevant personnel (including deputies) are exercised.

An organization’s BC capability cannot be considered reliable until it has been exercised. No matter how well designed a BC strategy or Business Continuity Plan (BCP) appears to be, robust and realistic exercises will identify issues and assumptions that require attention. To be successful an Exercise Programme should begin simply and escalate gradually in terms of complexity and challenge.

The aims of exercising include:
• Evaluating the organization’s current BC capability;
• Identifying areas for improvement or missing information;
• Highlighting assumptions which need to be questioned;
• Instilling confidence in exercise participants;
• Developing team work;
• Raising awareness of BC throughout the organization; and
• Testing the effectiveness and timeliness of restoration procedures.

The Exercise Programme should use a combination of techniques to ensure that the aims are achieved across the whole organization over a planned timescale.

The Exercise Programme should include suitable exercising of the following elements of the BCM programme:
• Technical – does all the required equipment work?
• Procedures – are the procedures and plans 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? and
• Personnel – are the right people involved and do they have the required skills, authority and experience? Does everyone know their role?

The frequency of exercising is dependent on the nature, scale and complexity of the organization. It is recommended that the Exercise Programme ensures that every member of the organization’s incident response (including deputies) should be involved in an exercise at least every 12 months.

Concepts and Assumptions
The organization’s BC policy and BCM programme management addresses how the Exercise Programme is to be planned and managed, specialist training undertaken and necessary resources identified.
ISO 22301:2012 defines an exercise as a process to train for, assess, practice and improve performance in an organization.

Exercising is a generic phrase used in the GPG that encompasses ‘testing’ which is a unique form of exercise with a pass or fail element, commonly utilised when testing equipment or technology. Exercises are used for validating policy, plans, training, communications, and for rehearsing the roles and responsibilities of teams and individuals.

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. It may be appropriate to consider inter-organizational exercising arrangements with interested parties. In addition, other suppliers of prioritized resources, products and services will have been identified in the Analysis stage of the BCM Lifecycle and should be asked to demonstrate their own recovery capability within the urgency of what they supply.

Methods and Techniques

Types of Exercise

There are many names given to different types of exercise ranging in scale and complexity, but in principle they fall into the following five categories.

• Discussion-based exercises

These exercises are considered to be the most cost effective and the least time consuming of exercise types. They are commonly structured events where participants can explore relevant issues and walk through plans in an unpressurised environment. This type of exercise can focus on a specific area for improvement that has been identified with the aim being to find a possible solution.

• Table top exercises

A Table top exercise is a type commonly used where the discussion is based on a relevant scenario with a time line which may run in ‘real time’ or may include ‘time-jumps’ to allow different phases of the scenario to be exercised. Participants are expected to be familiar with the plans being exercised and are required to demonstrate how these plans work as the scenario unfolds. Table top exercises can be a realistic, cost effective and efficient method. This type of exercise can be greatly enhanced by the use of media which can make a scenario more realistic.

• Command Post exercises

Command post exercises typically involve management teams at a strategic, tactical or operational level. Participants can be located across the whole organization (and could potentially involve willing interested parties), all working from their usual day to day locations. In these exercises, participants are given information in a way that simulates a real incident. Participants can be invited to respond as they would for real, they are expected to deal with the situations that they encounter, linking in to others as necessary. These exercises have the added advantage of testing information flow, communication and equipment, in addition to procedures, decision making and coordination.

• Live

Live exercises can range from a small scale rehearsal of one component of the response, for example evacuation,

Process

<table>
<thead>
<tr>
<th>• Review the scope (plans, recovery resources and activities) of past tests to identify areas not recently exercised;</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Discuss with Top Management any perceived areas of weakness and exercising priorities;</td>
</tr>
<tr>
<td>• Determine budget for the Exercise Programme;</td>
</tr>
<tr>
<td>• Decide on suitable types of exercise for the areas to be exercised over the planning period, perhaps for a year ahead;</td>
</tr>
<tr>
<td>• Check the availability of required personnel and facilities;</td>
</tr>
<tr>
<td>• Draw up a programme of exercises;</td>
</tr>
<tr>
<td>• Submit to Top Management for approval if required; and</td>
</tr>
<tr>
<td>• Identify any training requirement for exercise participants or planners and integrate into the Exercise Programme.</td>
</tr>
</tbody>
</table>
through to a full scale rehearsal of the whole organization and potentially participating interested parties. Live exercises are designed to include everyone likely to be involved in that part of the response. This type of exercise is particularly useful where there is a legal or regulatory requirement or where a high risk to an organization has been identified and the response and recovery plans need to be fully tested. They are considered to be the most appropriate and realistic way to train people and test plans. However, there are a number of challenges that by their nature might not always make a live exercise the most effective exercise format, for example; the resources required can be significant and there may be financial implications, care must be taken to avoid disruption to the normal operation of the organization and any reputational impact must be considered.

• Test

A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned. (ISO 22301:2012) It is usually applied to equipment, recovery procedures or technology, not to individuals, for example, the rebuilding of a server from back-up tapes within a set number of hours.

Outcomes and Review
The outcome is:

• An effective Exercise Programme; and

• Defined requirements for resources (including budget) and training for the Exercise Programme.

An organization’s Exercise Programme should be reviewed regularly to ensure it meets the objectives and that is it validating the effectiveness of the overall BCM Programme.

Developing an exercise

Introduction
Each exercise within the Exercise Programme needs to be carefully planned to maximise the benefits from the time expended in developing and delivering it.

Concepts and Assumptions
Realism: Exercises should feel as real as possible. They 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 practical to run certain exercises without alterations to “live” procedures. The usefulness of an exercise is reduced by the selection of an unrealistic scenario. Setting a realistic business scenario helps to ensure that the participants engage fully in the exercise and additionally benefit from the experience. The selection of a feasible scenario will also help prove the validity of plans. It is essential that the exercise facilitator works with facts to ensure participants gain the most from the exercise through the realism of the scenario and supporting material.

Increasingly technology developed by third parties is available to add realism. This often takes the form of games, which attracts maximum interest and involvement from previously disinterested staff. The introduction of external parties can add an air of uncertainty and create greater attention and interest in exercise participation.

Minimal Exposure: Exercising should focus on maximising business benefits while minimising the exposure to disruption. Unfortunately, exercising can sometimes be the cause of disruption to the organization, and it is important that those responsible for planning and managing exercises ensure:

• The chance of disruption caused by the exercise and the impact of any potential disruption is minimised; and

• The residual risk of something going wrong is understood and accepted by Top Management.

Costs and benefits: The cost of organising and running an exercise depends on the type of exercise selected. A more complex exercise is usually more expensive and may create more exposure to disruption; however it may give greater confidence in the effectiveness of the response.
**Preparation:** The scope and complexity of the exercise will determine the skills needed by the team designing and running the exercise. Members of the team should ideally have exercise design/delivery skills and know the organization or the business sector being tested.

Although it is often appropriate for in-house staff to develop and run exercises there are other options which involve the engagement of external parties. This might well be Emergency Services who may be willing to be involved in some basic exercises such as evacuation.

Whether internal or externally facilitated, an individual or team should be nominated to run the exercise. This individual (sometimes called an exercise manager) or team will manage the exercise in accordance with the exercise plan/schedule, initiating and controlling the various stages as they unfold.

**Participants:** Those involved in exercises may include:

- Facilitator(s);
- Observer(s);
- Strategic, Tactical, Operational level incident response teams as appropriate;
- Departmental BC Representatives;
- Suppliers of recovery resources and services;
- Emergency services;
- Local authority emergency planners;
- Subject matter experts; and
- Auditor(s).

Consideration should be given, if appropriate, to involving a wider interested party group including customers, suppliers, regulators, statutory/professional bodies, agencies, emergency services and the voluntary sector.

Inviting observers and the media to participate requires careful consideration. The advantages and disadvantages of allowing visitors to observe the exercise should be reviewed with Top Management and thought should be given to the organizational risks involved together with health and safety implications.

Although it is sometimes necessary to conduct an unannounced test, (for example, an out-of-hours call-out cascade), it is more common for exercises to be pre-announced to key participants so as to minimise the risk of the exercise causing disruption. The warning time and the number of pre-warned participants may reduce as the organisation becomes more confident in its BC capability.

**Process**

Although a range of different exercises are undertaken in the validation of the BCM programme, the following process can be used (to a varying degree depending upon complexity) for any individual exercise:

- Agree the scope, aims, objectives and expected outcomes of the exercise;
- Identify the exercise planning team;
- Design – plan and design the exercise, including setting a budget and conducting a risk assessment to identify the risks of an impact on live operations, where appropriate;
- Conduct – run the exercise;
- De-brief – assess and report the outcome, including a de-brief of the participants immediately after the exercise; and
- Follow-up – address any issues raised by the exercise.

**Methods and Techniques**

**Planning the exercise** - The schedule for an exercise should contain a chronological listing of events, with expected participant outcomes from each. The schedule links simulation to action and reflects each event that will prompt players to implement the procedure being validated. Individual scheduled events are commonly known as “injects” which can be delivered by the facilitator or various media.

Each inject should contain the following information:

- Exercise objective being met;
• Designated event timescale;
• Event description;
• Exercise team member delivering the inject;
• Participant responsible for event action; and
• Expected participant response.

Prior to the exercise starting: All participants should be aware of what is required of them during and immediately after the exercise. This can be achieved by way of written information in advance of the exercise and a briefing immediately before the exercise. It is essential the briefing does not adversely affect the intended aim of the exercise. Topics for the pre-exercise briefing may include:

• Exercise aims and objectives;
• Roles and responsibilities during the exercise;
• Information, communication and technology systems to be used;
• Action in the event of unforeseen circumstances; and
• Post exercise requirements.

It is essential participants and the wider organization are made aware that an exercise is taking place and that the incident is fictitious to prevent misunderstanding or increased organizational risk.

If the exercise calls for a no notice or limited notice trigger for the exercise, participants should be briefed as soon as possible after the exercise starts that they are taking part in an exercise and that the scenario is fictitious.

Starting the exercise: Triggering the start of the exercise should be clear and unambiguously communicated to all participants and usually comes in the form of an inject.

During the exercise: Activities should occur in a predetermined way as outlined in the exercise plan and schedule.

Suspending the exercise: It may be necessary to pause or stop an exercise. Participants need to be made aware of a code word which will prompt a suspension. This should be a word not usually used within the work environment. The exercise may have to be stopped if participant safety is, or could be, compromised, or where a real incident has occurred.

For complex exercises, those responsible for planning and managing the exercise should ensure that there are agreed stop/go points at key stages throughout if the team is making decisions that would not be appropriate in the given scenario, and there are adequate back-out plans in case of things going wrong. Taking time out can be a useful tool to discuss a series of exercise occurrences to gain learning, or to address a significant deviation from an expected participant action which could, if not rectified, affect the continuance of the exercise.

Following a suspension, the exercise could be restarted or terminated.

Ending the exercise: The decision to end the exercise should rest with the individual or team managing the exercise. Consideration should be given as to whether the exercise objectives have been completed and the allocated time period for the exercise.

Sufficient time should be allowed for an immediate debrief to take place.

Debriefing: The aim of exercise debriefing is for participants to communicate their experiences of an incident so that lessons can be identified and incorporated into the BCM programme. Plans, procedures and training can then be modified to reflect lessons identified and therefore improve the organization’s ability to respond to future BC disruptions.

This style of debrief should not be confused with a therapeutic debrief used following a real world incident to identify and deal with participant psychological trauma. It is vital that all staff involved, regardless of seniority, understand that debriefing is about improving effectiveness and not about assigning blame.

All staff participating in the exercise should be given the opportunity to contribute to the debriefing process.

Exercise debriefing should be carried out in a manner conducive to promoting organizational learning and
encouraging open and honest feedback.

Debriefing should:

• Respect the rights of individuals;
• Value equally all those participating; and
• Pursue individual, group or organizational understanding and learning.

There are two main types of exercise debrief:

• **Hot debrief** - this is held immediately after an exercise prior to staff leaving the exercise location and allows the participants the opportunity to highlight a variety of issues and concerns while fresh in their minds; and

• **Formal debrief** - this should be within weeks of the exercise taking place and should address the wider organizational issues rather than individual or group concerns. It should look for strengths and weaknesses as well as ideas for future learning.

**Post exercise report:** The results of the debriefing should be used to prepare a post exercise report and recommendations.

To ensure any lessons identified become lessons that are learnt, the post exercise report should be distributed to all relevant staff and interested parties.

It is essential there is a management process to feed the findings of the post exercise report into the maintenance activity and an action plan should be created to implement the recommendations which may require changes to the BCM Programme.

Consideration should be given to re-running an exercise, after corrective actions have been put in place, where significant issues had been identified.

**Outcomes and review**

Consideration should be given at an early stage to identifying how the exercise objectives (success or failure) will be measured and by whom. An effective way of achieving this is to identify a number of objective performance indicators which describe when objectives have been met or not.

**Examples of expected outcomes from an exercise may include:**

- First responder to use the alert, invocation and escalation process;
- On-duty manager to activate the callout procedure for the incident management team;
- Convene an initial incident management meeting;
- Maintain an incident log;
- Develop an incident management structure as defined within the BCP;
- Allocate roles and responsibilities as per the BCP; and
- Establish lines of communication with interested parties.

The wider outcomes of the exercise may include:

- Validation that the BC Programme is effective;
- Confirmation that team members and staff are familiar with their roles, responsibilities and authority in response to an incident;
- Validation of the technical, logistical, administration aspects of the BCP;
- Confirmation of the recovery infrastructure (command centres, work areas, technology and telecommunications resource recovery);
- Confirmation of the availability of staff and processes for relocation;
- Documentation of exercise results in a post exercise report for Top Management, auditors, insurers, legal bodies and regulators as appropriate;
- Documentation and resolution of issues identified during the exercise;
- An increased awareness of emergency procedures;
- An increased awareness of the significance of BC;
Process
A formal process for maintaining the BCM programme needs to be established. The process should be undertaken at planned intervals, the frequency of which will depend on the nature and expected pace of change in the activity being maintained. For example, the plans containing contact details may need to be maintained every month, whereas maintenance of the BC Policy can probably be scheduled once a year. Responsibility for undertaking the planned maintenance process should be given to an individual or team, and consists of:

• Review what has changed since the last update;
• Analyse the impact of any changes;
• Update the plans as required;
• Identify any knock-on changes to other areas;
• Advise those responsible in other areas of the knock-on changes;
• Assess whether changes and amendments create a training programme, awareness campaign and/or communication need;
• Provide training, awareness and/or communications as required;
• If plans have been changed, distribute the new versions as appropriate;
• Identify the date for undertaking the next planned maintenance, and schedule the maintenance.

The analysis of the impact of any changes should include:

• Reviewing and challenging any assumptions that have been made;
• Determining whether any time objectives have changed;
• Determining the adequacy and availability of external services that might be required, such as asset restoration, recovery sites and subcontracts; and
• Reviewing the Business Continuity arrangements of key suppliers.

Maintenance
Introduction
Maintenance of the BCM programme keeps the organization’s BC arrangements up to date, ensuring that the organization remains ready to respond to manage incidents effectively, despite constant change. An important part of the BCM Lifecycle is to manage the documentation, and maintenance of the BCM programme ensures that this documentation is kept up to date and that current and relevant documentation is distributed to appropriate interested parties.

General Principles
To be effective, maintenance activities should be embedded within the organization’s normal management processes rather than be a separate activity that can be ignored or forgotten. As much of the maintenance required will be the result of internal changes within the organization, the most effective way of achieving this is to incorporate maintenance activities into the organization’s change management process. However, this is not always possible as many organizations do not have such a process. Maintenance activities are identified through:

• Lessons learned through exercising;
• Changes in the environment in which the organization operates;
• A review, particularly an audit;
• A real incident, when lessons learned can be incorporated; and
• Updated or changed BIA outputs.

Although the need for maintenance will be triggered by any or all of the above, regular and planned maintenance is required for the entire BCM programme, as described throughout these Good Practice Guidelines.
**Methods and Techniques**

Responsibility for maintenance should be given to those who have local responsibility for BC, although plan distribution can be handled by a central individual or team. For example, a BC departmental representative can be made responsible for updating their plan and dynamic data such as staff out-of-hours contact numbers, team tasks, notification and supplier contact details as well as battle box contents, and for sending the updated plan to a central point for distribution. To be effective, updated documentation should be distributed under a formal change control (version) process.

If it is to achieve its purpose, maintenance needs to be managed. This requires the production of regular reports identifying progress in planned maintenance, highlighting areas of weakness, and making recommendations for improving the process. Proprietary software can be very effective in managing documentation in that many such systems contain follow-up, tracking, reporting and reminders to ensure that planned maintenance takes place as and when planned.

**Outcomes and Review**

The outcomes of maintenance of the BCM programme include:

- A documented planned maintenance schedule;
- Regular progress reports;
- Effective and current policies and procedures;
- Up to date documentation; and
- Distribution to appropriate interested parties.

Successful maintenance of the BCM programme should be formally reviewed at least once a year, and changes made where necessary for continual improvement.

**Review**

**Introduction**

The purpose of Review is to evaluate the BCM programme and identify improvements to both the organization’s implementation of the BCM Lifecycle and its level of organizational resilience.

There are five basic types of review:

- **Audit** (internal and external) – a formal impartial review process that measures an organization’s BCM programme against a pre-agreed standard;
- **Self-Assessment** – an assessment of the organization’s BCM programme by itself;
- **Quality Assurance** (QA) – a process that ensures that the various outputs from the BCM programme meet requirements;
- **Performance Appraisal** – a review of the performance of individuals tasked with BC roles and responsibilities; and
- **Supplier Performance** – a review of a key supplier’s BCM programme or a review of the performance of a supplier of recovery services.

**General Principles**

**Audit**

Auditing is designed to verify that the process has been followed correctly, not that the solutions adopted are necessarily correct. ISO 22301:2012 defines audit as a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

A BCM audit has five key functions:

- To validate compliance with the organization’s BC policies and standards (includes any legislation or regulations) or;
- To review the organization’s BCM programme;
- To validate the organization’s BCP;
- To verify that appropriate exercising and maintenance activities are taking place; and
- To highlight deficiencies and issues and ensure their resolution.

The audit process should be conducted on a regular basis as defined by the organization’s audit and governance policies. It is recommended that the period between audits should not exceed 2 years, which is in line with that...
expected by standards bodies. The audit should be conducted against a BC Policy and appropriate standards identified by it. The purpose of a BCM audit is to scrutinise an organization’s existing BCM programme; verify it against predefined standards and criteria and deliver a structured audit opinion report.

Self-Assessment
The purpose of self-assessment is for an organization to review its implementation of the BCM programme, with a view to creating an action plan for improvements. Self-assessment can be carried out between audits to identify progress against audit recommendations. Self-assessment should also be carried out during and immediately after an initial implementation of the BCM programme.

Quality Assurance
Quality Assurance is the process of determining whether the outputs from the BCM programme meet the organization’s requirements and expectations, which may or may not have been formally defined. For organizations that are certified against International or national standards, this will be a formal and documented process. For other organizations this will most likely take the form of an informal review against expectations.

Performance Appraisal
Roles and responsibilities for BC will have been defined as part of BC Policy. Performance appraisals should be used to check how well those roles and responsibilities are being performed.

Supplier Performance
The review of the BCM programme of any supplier on which the organization depends should be similar to those employed for reviewing the organization’s own programme. The performance of suppliers of recovery services should be reviewed on a regular basis.

Concepts and Assumptions
Audit
An audit assumes that if the process is correct and properly applied then the outcome should provide evidence of an effective BCM programme. It also assumes that the standard adopted by the organization is effective and provides a suitable framework for audit. The assessment method adopted by the organization will have been defined in its BC Policy document and can be an internationally or nationally recognised standard such as ISO 22301:2012, or an in-house approach developed by the organization itself (possibly based on these Good Practice Guidelines), or a mandatory requirement imposed on the organization by legal or regulatory requirements.

Self-Assessment
Self-assessment assumes that an organization has identified objectives and targets against which its BCM programme can be assessed.

Quality Assurance
Quality Assurance assumes that the requirements for the outputs from the BCM programme have been identified.

Performance Appraisal
Performance appraisal assumes that the roles and responsibilities for BC have been defined.

Supplier Performance
Supplier Performance assumes that the suppliers on which the organization depends have been identified, and the expectations of their BCM programme defined.
Process

Audit
The BCM audit is concerned with a complex process and requires interaction with a wide range of managerial and operational roles from both business and technical perspectives.

The BCM audit process includes:

- Developing a BCM audit plan;
- Defining the audit scope;
- Defining the audit approach;
- Reviewing information gathered by the BCM audit activities;
- Compiling and summarising interview notes, questionnaires and other sources;
- Identifying gaps in content and level of information gathered then conducting follow up interviews as appropriate;
- Obtaining and comparing relevant documentation e.g. BIA with interview data and other sources e.g. walkthrough, physical inspection, sampling;
- Reference to secondary sources e.g. standards, regulations, legislation and ‘good practice’ guidelines to validate preliminary findings;
- Forming 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;
- Providing a draft audit opinion report for discussion with key interested parties;
- Providing an agreed audit opinion report incorporating recommendations as well as audited responses where differences of opinion persist;
- Providing an agreed remedial action plan including timescales to implement the agreed recommendations of the audit report (this should also form a key element of the BCM Programme); and
- Providing a monitoring process to ensure that the audit action plan to address material deficiencies is implemented within the agreed timescale.

Self-Assessment
The self-assessment process should include:

- Identifying objectives or measures for the BCM programme against which performance can be assessed;
- Reviewing performance against the selected objectives or measures;
- Identifying trends in performance;
- Highlighting areas for improvement;
- Developing action plans to improve these areas; and
- Producing a self-assessment report.

Quality Assurance
Quality Assurance can be undertaken as a continual process on all outputs, or through periodic sampling. The process involves:

- Identifying requirements or expectations;
- Comparing the output to its requirements or expectations;
- Identifying any shortfall in requirements or expectations; and
- Taking action to remedy any shortfall.

Persistent failure to meet requirements should be addressed by changes in the processes, procedures, or resources used to produce the outputs.

Performance Appraisal
The performance appraisal process can be undertaken as part of a regular staff appraisal process, or just to review an individual’s performance in their BC role.

The process involves:

- Confirming the individual’s BC role and responsibilities;
- Defining Key Performance Indicators (KPIs) for the role (objectives, measurement targets and standards); and
- Defining success factors for the KPIs;
• Incorporating KPIs in annual appraisals;
• Evaluating and reviewing performance against KPIs;
• Producing KPI performance scores; and
• Providing a remedial action plan to remedy any shortfall in performance.

Supplier Performance
The process for reviewing the BCM programme of key suppliers and reviewing suppliers of recovery services should be defined by contract. The BCM programme of key suppliers should be reviewed as if they were part of the organization itself, in the same way that the BC arrangements of any internal department, location, or subsidiary that provides products and services on which the organization depends would be reviewed.

Methods and Techniques

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

A BCM audit plan should include identification of the:

• Type of audit to be carried out e.g. compliance, project management/control, feasibility study, due diligence or investigative;

• Audit objectives, which in part might be driven and governed or restricted by legal or regulatory requirements. This includes key issues of high priority; and

• Standard audit framework (where appropriate) to be used. The audit framework may be governed or restricted by legal or regulatory requirements.

The definition of the audit scope should include determining the:

• Corporate governance, compliance or other issues to be audited; and

• Area/department/site of the organization to be audited.

The definition of the audit approach should include:

• 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); and

• Determine the requirement for specific subject expertise or third party assistance to conduct the audit.

Forming of an opinion could include:

• 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.

Self-Assessment
Objectives or measures to be used in self-assessment could include such things as:

• Project milestones for the BCM programme;

• Percentage of plans maintained by the scheduled date;

• Percentage of members of response teams involved in an exercise each year;

• Number of lessons learned from exercises still not addressed; and

• Extent of the completion of the BIAs against scope.

Quality Assurance
Requirements can be identified through reviewing the BCM programme, but identifying expectations will involve interviewing staff and interested parties. Comparing BCM programme output to requirements or expectations and identifying shortfalls:

• Does a document conform to the document control standards?

• Has a plan been verified by its owner?

• Does a BIA identify the MTPDs of all the urgent activities?

• Have the resources required to recover an activity been identified?

• Have the recommended strategies and tactics been agreed by Top Management?
• Does the BCP have an agreed scope signed off by Top Management?

Performance Appraisal
KPIs could include such things as:

• Number of times scheduled plan maintenance dates were met;
• Percentage completion of the BIA;
• Number of exercises undertaken as planned;
• Number of plans completed;
• Number of outstanding issues resulting from incidents, exercises and audit; and
• Expenditure against budget.

Supplier Performance
Supplier performance should be reviewed against contractual Service Level Agreements (SLAs), which in the case of key suppliers should relate to their BCM programme.

Outcomes and Review
The outcome should be an improvement in the organization’s level of resilience, and one or more action plans for further improvement.

Each element of the Review process itself should be reviewed on an annual basis, and an action plan for improving the process should be produced.

Audit
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 plans by management as ‘inadequate’; and
  ▶ The initiation of a review conducted by a BC professional to assist the team in improving their position.

Self-assessment
The outcomes of self-assessment include:

• An action plan for improvements;
• An improvement in the BCM programme; and
• An improvement in the organization’s level of resilience.

Quality Assurance
The outcome of Quality Assurance should be:

• An improvement in the way the outputs from the BCM programme meet the organization’s requirements and expectations.

Performance Appraisal
The outcome of a Performance Appraisal should be an improvement in the way in which an individual tasked with a BC role:

• Carries out their role;
• Undertakes their responsibilities; and
• Meets their objectives.

Supplier Performance
The outcomes of reviewing supplier performance include:

• A performance rating against SLAs;
• An understanding of the supplier’s BCM programme; and
• An action plan for improving supplier performance.

Conclusion
Validation is the final stage of the BCM Lifecycle. It is important that the Maintenance and Review of the BCM programme is ongoing. The stages of activity and the six Professional Practices covered in these Good Practice Guidelines have the overall aim of improving organizational resilience. The BCI offer training and certification for individuals and organizations on the practical aspects of these guidelines. Please visit www.thebci.org for more information.
# Glossary

## Table Key

| ISO terminology accepted by the BCI and referenced in the GPG | Red |
| Good Practice Guidelines Terminology | Amber |
| Defined outside of Business Continuity | Blue |

*BCI Dictionary is a consolidation of terms and definitions that exist throughout the world. Visit [www.thebci.org](http://www.thebci.org) for the latest version.*

<table>
<thead>
<tr>
<th>Term</th>
<th>Abbreviation</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td></td>
<td>A process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products and services.</td>
<td>BS ISO 22301:2012</td>
</tr>
<tr>
<td>Analysis</td>
<td>PP3</td>
<td>The Technical Practice within the BCM Lifecycle that reviews and assesses an organization in terms of what its objectives are, how it functions and the constraints of the environment in which it operates.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Associate Member Business Continuity Institute</td>
<td>AMBCI</td>
<td>Statutory Membership level of the Business Continuity Institute - a professional certification. For Business Continuity Professionals with at least one year’s experience.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Audit</td>
<td></td>
<td>Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>BC Policy</td>
<td></td>
<td>The key document that sets out the scope and governance of the BCM programme and reflects the reasons why it is being implemented</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>BC Professional</td>
<td></td>
<td>An experienced individual with responsibilities for practising and/or managing Business Continuity. The BCI consider a BC professional to be an individual who is certified to the Membership level AMBCI or above.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>BCI Global Membership Council</td>
<td>GMC</td>
<td>An international group of Business Continuity professionals elected to represent BCI Members worldwide.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Term</td>
<td>Abbreviation</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>BCM Lifecycle</td>
<td></td>
<td>The stages of activity that an organization moves through and repeats with the overall aim of improving organizational resilience.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>BC</td>
<td>The capability of the organization to continue delivery of products or services at acceptable redefined levels following a disruptive incident.</td>
<td>ISO 22300</td>
</tr>
<tr>
<td>Business Continuity Institute</td>
<td>BCI</td>
<td>The BCI is a Global Membership Institution for Business Continuity Professionals. The overall purpose is to promote the art and science of business continuity worldwide.</td>
<td>BCI</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>BCM</td>
<td>A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Business Continuity Management programme</td>
<td></td>
<td>Ongoing management and governance process supported by Top Management and appropriately resourced to implement and maintain business continuity management. (This is the ISO definition for ‘business continuity programme’.)</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Business Continuity Management System</td>
<td>BCMS</td>
<td>Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Business Continuity Plan</td>
<td>BCP</td>
<td>Documented procedures that guide organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td>BIA</td>
<td>Process of analysing activities and the effect that a business disruption might have on them. (Note: The GPG 2013 recommends that this is a four stage process, starting with an Initial BIA followed by Strategic, Tactical and Operational level BIA’s.)</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Certificate of the BCI Examination</td>
<td>CBCI</td>
<td>The BCI Examination leading to the post-nominal designation CBCI, a recognised industry credential.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Term</td>
<td>Abbreviation</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Competence</td>
<td></td>
<td>Ability to apply knowledge and skills to achieve intended results.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Continual improvement</td>
<td></td>
<td>Recurring activity to enhance performance.</td>
<td>ISO 22300:2012</td>
</tr>
<tr>
<td>Corrective action</td>
<td></td>
<td>Action to eliminate a detected nonconformity.</td>
<td>ISO 22300:2012</td>
</tr>
<tr>
<td>Crisis</td>
<td></td>
<td>A situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organization and requires urgent action.</td>
<td>ISO 22300:2012</td>
</tr>
<tr>
<td>Design</td>
<td>PP4</td>
<td>The Technical Practice within the BCM Lifecycle that identifies and selects appropriate strategies and tactics to determine how continuity and recovery from disruption will be achieved.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Diploma of the Business Continuity Institute</td>
<td>DBCI</td>
<td>The BCI Diploma is an academic qualification leading to the post-nominal designation of DBCI.</td>
<td></td>
</tr>
<tr>
<td>Disruption</td>
<td></td>
<td>See ‘Incident’.</td>
<td></td>
</tr>
<tr>
<td>Diversification</td>
<td></td>
<td>A continuity and recovery strategy requiring the live undertaking of activities at two or more geographically dispersed locations.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Embedding Business Continuity</td>
<td>PP2</td>
<td>The Management Practice within the BCM Lifecycle that continually seeks to integrate Business Continuity into day-to-day activities and organizational culture.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Exercise</td>
<td></td>
<td>A process to train for, assess, practice and improve performance in an organisation.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Exercise programme</td>
<td></td>
<td>Series of exercise events designed to meet an overall objective.</td>
<td>ISO 22300:2012</td>
</tr>
<tr>
<td>Fellow of the Business Continuity Institute</td>
<td>FBCI</td>
<td>Statutory Membership Level of the Business Continuity Institute for professional certification. The highest attainable level of BCI Membership, for very experienced and active BCI Members.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Term</td>
<td>Abbreviation</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Formal Debrief</td>
<td></td>
<td>A discussion held within weeks of the exercise, addressing the wider organizational issues that identifies learning opportunities.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Hot Debrief</td>
<td></td>
<td>A discussion about the issues and concerns held immediately following an exercise.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Implementation</td>
<td>PP5</td>
<td>The Technical Practice within the Business Continuity Management (BCM) Lifecycle that executes the agreed strategies and tactics through the process of developing the Business Continuity Plan (BCP).</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Incident</td>
<td></td>
<td>Situation that might be, or could lead to, a disruption, loss, emergency or crisis. (Note: The GPG 2013 also refers to an incident as an event, interruption or disruption.)</td>
<td>ISO 22300:2012</td>
</tr>
<tr>
<td>Interested party stakeholder</td>
<td></td>
<td>Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Invocation</td>
<td></td>
<td>Act of declaring that an organization’s business continuity arrangements need to be put into effect in order to continue delivery of key products and services.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Maximum Tolerable Period of Disruption</td>
<td>MPTD</td>
<td>The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing and activity, to become unacceptable.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Member of the Business Continuity Institute</td>
<td>MBCI</td>
<td>Statutory Membership level of the Business Continuity Institute - for professional certification. For experienced Business Continuity professionals with at least three years' experience.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Minimum Business Continuity Objective</td>
<td>MBCO</td>
<td>A minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Term</td>
<td>Abbreviation</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Organization</td>
<td></td>
<td>Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Organizational culture</td>
<td></td>
<td>The combined assumptions, beliefs, values and patterns of behaviour that are shared by members of an organization. The way in which an organization views itself, its place in its market and the environment in which it operates.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Organizational Resilience</td>
<td></td>
<td>The capability to anticipate key events from emerging trends, constantly adapt to change and to bounce back from disruptive and damaging incidents.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Outsourced Activities</td>
<td></td>
<td>Those processes that are performed by, or in part by, a third party.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Policy and Programme Management</td>
<td>PP1</td>
<td>The first stage of the BCM Lifecycle. It is the Professional Practice that defines the organizational policy relating to Business Continuity and how that policy will be implemented, controlled and validated through a BCM programme.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Post incident acquisition</td>
<td></td>
<td>A continuity and recovery strategy where resources are provided following an incident at short notice.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Process</td>
<td></td>
<td>A set of interrelated or interacting activities which transforms inputs to outputs.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Products and services</td>
<td></td>
<td>Beneficial outcomes provided by an organization to its customers, recipients and interested parties.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Professional Practices</td>
<td>PPs</td>
<td>The activities that make up the six stages of the BCI’s Good Practice Guidelines BCM Lifecycle.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Recovery Point Objective</td>
<td>RPO</td>
<td>The point to which information used by an activity must be restored to enable the activity to operate on resumption. Also referred to as Maximum Data Loss.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Recovery Time Objective</td>
<td>RTO</td>
<td>The period of time following an incident within which a product or an activity must be resumed, or resources must be recovered.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Term</td>
<td>Abbreviation</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Replication</td>
<td></td>
<td>A continuity and recovery strategy where resources are copied to a dormant site, only being brought into live operations after an incident.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Resilience</td>
<td></td>
<td>Adaptive capacity of an organization in a complex changing environment.</td>
<td>ISO Guide 73</td>
</tr>
<tr>
<td>Risk</td>
<td></td>
<td>Effect of uncertainty on objectives</td>
<td>ISO Guide 73</td>
</tr>
<tr>
<td>Risk assessment</td>
<td></td>
<td>Overall process of risk identification, risk analysis and risk evaluation.</td>
<td>ISO Guide 73</td>
</tr>
<tr>
<td>Risk Management</td>
<td>RM</td>
<td>Coordinated activities to direct and control an organization with regard to risk.</td>
<td>ISO Guide 73</td>
</tr>
<tr>
<td>Safe separation distance</td>
<td></td>
<td>An adequate geographical spread between the original and duplicate resources, the various suppliers, the replica operations or the base site and its recovery site.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Standby</td>
<td></td>
<td>A continuity and recovery strategy where a facility is available to be made operational as required.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Subcontracting</td>
<td></td>
<td>A continuity and recovery strategy where third parties are used to produce a product or service, provide process infrastructure and undertake activities.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Technical Practices</td>
<td></td>
<td>The Analysis, Design, Implementation and Validation stages of the BCM Lifecycle.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Test</td>
<td></td>
<td>A unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.</td>
<td>ISO 22301:2012</td>
</tr>
<tr>
<td>Threat</td>
<td></td>
<td>Potential cause of an unwanted incident, which can result in harm to individuals, a system or organization.</td>
<td>ISO 22300:2012</td>
</tr>
<tr>
<td>Threat Analysis</td>
<td></td>
<td>The process of evaluating threats to identify unacceptable concentrations of risk to activities and single points of failure.</td>
<td>GPG 2013</td>
</tr>
<tr>
<td>Top Management</td>
<td></td>
<td>Person or group of people who directs and controls an organization at the highest level.</td>
<td>ISO 22301</td>
</tr>
<tr>
<td>Validation</td>
<td>PP6</td>
<td>The Technical Practice within the BCM Lifecycle that confirms that the Business Continuity Management (BCM) programme meets the objectives set in the Business Continuity (BC) Policy and that the organization’s Business Continuity Plan (BCP) is fit for purpose.</td>
<td>GPG 2013</td>
</tr>
</tbody>
</table>
Membership of the Business Continuity Institute says more about a business continuity professional than anything else. It says that they are both knowledgeable and experienced; have a keen interest in their subject with the willingness to stay on top of current thinking; have a true professional approach to their discipline and enjoy being part of a global practitioner community.

The BCI is like no other BC Institute – we are a membership body sharing best practice, inspiring thought leadership and pushing new ideas and developments within the discipline. Salary research studies have shown that BCI members are better compensated than members of other Institutes.

Established in 1994, the BCI operates on the following principles:

**OUR PURPOSE**
- To promote the art and science of Business Continuity worldwide

**OUR VISION**
- To be the Institute of choice for Business Continuity professionals

**OUR VALUES**
- Membership Focused – where our members are at the heart of everything we do
- Quality Led – consistently delivering a high value, independent service
- Global Reach – building a worldwide community of influential thought leaders

**OUR GOALS**
- To deliver a consistent ‘BCI experience’ for members to develop and enhance their qualifications and expertise
- To strengthen BCI’s role as ‘the global thought leader’ for BC
- To increase BCI’s global influence within both mature and emerging BC markets

Entry requirements: CBCI® or DBCI is needed to join the BCI in one of our Statutory grades of Associate Member (AMBCI) or Member (MBCI) with supporting evidence of practical experience as a business continuity practitioner.

* alternative credentials may be substituted see the BCI website for details
The BCI offers world-class, high-quality training, delivered by BCI licensed training partners located around the globe. All our training partners are experienced and respected business continuity professionals, bringing a wealth of real-life experience to their students.

1. Based on the BCI’s Good Practice Guidelines, which are the comprehensive and independent body of knowledge for business continuity (BC).
2. Designed to meet the current and future needs of business continuity professionals worldwide.
3. Delivered by a global network of BCI licensed training partners.
4. Enables students to study for an internationally recognised credential in business continuity (CBCI).
5. Develop specialist skills to improve expertise in BC.

**ENTRY LEVEL LEARNING**

The BCI Good Practice Guidelines Training course to support learning for the CBBCI credential (Certificate of the Business Continuity Institute)

**FIVE DAY OR THREE (EXTENDED) DAY OPTIONS AVAILABLE**

Classroom based – Instructor led
- This course provides an in-depth study of the Business Continuity Management (BCM) lifecycle. The subject matter addresses the six BCM Professional Practices as defined in the GPG, including Technical and Management Practices, taking the candidate through each stage of the BCM Lifecycle step by step. Using case studies and examples based on real-life experience, the instructors provide practical insights into all aspects pertaining to the development, implementation and management of a BC programme within an organization.

**LIVE ONLINE – 32 HOURS ACROSS EIGHT WEEKS**

Online – Instructor led
- Identical content to the classroom version but delivered in a more flexible way allowing the student to remain at work and save travel costs.

**SPECIALIST SKILLS TRAINING**

Entry level training takes the student through ‘what’ needs to be done to introduce business continuity into an organization. BCI Specialist Skills courses delve into the ‘how’ and show students what’s involved in delivering business continuity in the following areas:
- Business Impact Analysis Course
- Exercise Planning Course
- Crisis and Incident Management Course
- Supply Chain Continuity Management Course
- Writing Business Continuity Plans Course
- BCMS Audit Course

This portfolio of BC training is being extended with more courses being added.
About BCI Corporate Partnership

The BCI Corporate Partnership enables organizations to work more closely with the BCI to help raise the profile of Business Continuity management as a discipline within their organization and to promote the highest standards of professional competence in BC in organizations working in any sector worldwide.

The BCI Corporate Partnership campaigns to ensure that BC is viewed and adopted as a key management discipline in private, public and not-for-profit sectors.

**Benefits of BCI Corporate Partnership**

The key benefit of BCI Corporate Partnership is to enable organizations to register staff members who have BC responsibilities, either full time or as part of other roles, as Partner Affiliates. These Partner Affiliates have access to BCI member benefits including:

- publications
- research reports
- discounts on BCI and other events
- a wide range of other BC resources
- networking with other BC professionals

Corporate partnership annual fees start at £750 for smaller organizations rising to £3000pa for larger organizations.

**Reaching the BCI Audience**

BCI Corporate Partners, who are also vendors, are able to add a sponsorship package to their partnership to create a marketing channel to BCI members and the wider business continuity community through the wide range of BCI communications including print and digital media. A BCI Account Manager will be available to help plan a bespoke marketing strategy to maximize sponsorship opportunities for our Sponsoring Partners.
The BCI Certificate is a stand-alone credential leading to the CBCI – Certificate of the Business Continuity Institute. The BCI Certificate examination tests a candidate’s knowledge of the prescribed Body of Knowledge which, in this case, is the BCI’s Good Practice Guidelines.

Approaching 3000 candidates have taken the two-hour multiple choice examination for this Certificate, the majority of which have progressed to join the Institute as either an Associate Member (AMBCI) or Member (MBCI) after demonstrating sufficient practical business continuity experience to support their theoretical knowledge.

The CBCI is valid for three years, during which time an annual maintenance fee is payable, after which time it is necessary to resit the examination to demonstrate currency of knowledge.

Most candidates choose to take BCI Training to support their learning as they prepare for the examination and sit the exam at the end of the training course while the knowledge is still fresh in their minds. Other candidates select the self-study route and register to sit the exam at one of the internationally available Computer Based Testing centres.

New from the BCI working in partnership with Buckinghamshire New University

The BCI Diploma is a stand-alone academic qualification leading to the DBCI – Diploma of the Business Continuity Institute. Successful students may use their DBCI to apply to join the BCI as either an Associate Member (AMBCI) or Member (MBCI) after demonstrating sufficient practical business continuity experience to support their theoretical knowledge.

The BCI Diploma is delivered by distance learning across three 10 week modules.

**MODULE ONE**
Module One explores the history and context of business continuity management and is based on the Good Practice Guidelines (GPG), the comprehensive and independent view of current thinking in business continuity. This module provides an in-depth study of the Business Continuity Management (BCM) Lifecycle, allowing students the opportunity to develop a thorough understanding of current business continuity practices.

**MODULE TWO**
Module Two provides the platform for a more academic study and analysis of the BCM Lifecycle as well as an in-depth study of current and future resilience issues faced by organizations worldwide.

**MODULE THREE**
Module Three is a project-based research project. Students are required to propose and agree a research topic on a business continuity management or related topic with their tutor. Evidence of extensive research is required to support the project. Students are expected to submit a 5,000 words report that is assessed as part of the BCI Diploma award process.