

Good Practice Guidelines 2013 Global Edition Edited Highlights

A Guide to Global Good Practice in Business Continuity

Business Continuity Institute

www.thebci.org

Contents of Edited Highlights

Acknowledgments

The 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 educational programs.

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-upon 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 program 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 recognizes 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-upon 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 recognized 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 full 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 full 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 in the full version of the Good Practice Guidelines.

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, 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.

BC	Business Continuity	The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
BCM	Business Continuity Management	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.
BCMS	Business Continuity Management System	Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

SOURCE: ISO 22301:2012

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

PP1 Policy & Program Management

PP2 Embedding Business Continuity

Technical Practices

PP3 Analysis

PP4 Design

PP5 Implementation

PP6 Validation

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 recognizes 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 Program 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 programs 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 specialized.

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 recognized "gap" in adoption among smaller businesses. There is nothing inherently "corporate" about BC; however, the BCI recognizes 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 IT 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”.

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-upon 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 BCMS 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 Center 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 Programs 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 recognized third party audit of a BCM Program.

Evidence of a person's competence to conduct an externally recognized Audit would be the possession of an Audit qualification approved by the US IIA (Institute of Internal Auditors), or the 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.

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 Program. A risk management program should identify catastrophic threats that are outside of the organization's control and a BCM Program is one way to reduce the impact of such events.

When an organization implements a BCM Program 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 Program 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 Program 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 Program, 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 Program.

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 characterized 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".

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

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 Program.

Traditionally, incident management has been associated with the activation of and liaison with the Emergency response organizations, whereas emergency management itself has been seen as the domain of "first responder organizations" such as police, fire, ambulance, and local authorities. Although not universally true, the perception remains that most emergency management activities occur within the public sector, although high physical risk businesses such as oil and gas, chemicals and nuclear energy 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 recognized standardization 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 formalized method of ensuring that the organization's program is effective and aligned to its culture and requirements. Certification of a BCM Program 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 IT, the armed forces or the emergency services, new entrants to the profession come from management consulting, information assurance, risk and insurance, compliance and quality. Further, with 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 program 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 Program 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 a BCM Program will therefore differ from organization to organization reflecting its business and operating model.

Is a dedicated BC professional essential to manage the BCM Program?

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 recognized 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 specialized BC professional function to manage projects, co-ordinate plan developments, organise exercises and tests and validate the BCM Program.

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 Program - 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 Program. For example, the consequences of the globalization 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 Program 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 Program 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 Program.

• **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-upon 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 Program meets the objectives set in the BC Policy and that the organization's BCP is fit for purpose.

The BCM Lifecycle:
Improving organizational resilience

PP1- Policy and Programme Management

"Policy and Program 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 Program.

The Business Continuity Institute (BCI) considers that the BCM Program needs to operate at three different levels:

1	**Strategic**	decisions are made and policy is determined;
2	**Tactical**	operations are co-ordinated and managed; and
3	**Operational**	activities are undertaken

The principles, concepts and assumptions and detailed processes including methods and techniques and outcomes of this professional practice are described in the full version of the Good Practice Guidelines. The following activities are covered:

- Setting Business Continuity Policy;
- Determining the scope of the BCM program;
- Defining Governance for the BCM program;
- Implementing a BCM Program;
- Assigning roles and responsibilities, including skills required by those involved;
- Project and Program Management;
- Managing outsources activities;
- Managing supply chain continuity;
- Managing documentation, and
- Practical implementation considerations.

PP2 - Embedding Business Continuity

Embedding Business Continuity is one of the ongoing activities resulting from the BCM Policy and Program 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.

The principles, concepts and assumptions and detailed processes including methods and techniques and outcomes of this professional practice are described in the full version of the Good Practice Guidelines. The following topics are covered:

- Developing a culture of Business Continuity awareness;
- Skills and competence requirements;
- Managing a training program; and
- Managing an awareness campaign.

PP3 – Analysis

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

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.

The Business Impact Analysis

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.

The different types of BIA described in the full version of the Good Practice Guidelines 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 and the
- **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.

PP4 – Design

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 Program 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.

The section of the Good Practice Guidelines describes how to design and select continuity and recovery strategies and tactics and the importance of relating these to recovery objectives. These include options such as:

- Diversification
- Replication
- Post-incident acquisition, or
- Do nothing.

Threat Mitigation measures are targeted at unacceptable concentrations of risk, single points of failure and the main threats to the organizations' most urgent activities, all of which are identified and prioritized in the Analysis stage of the BCM Lifecycle.

The Incident response structure is designed to ensure 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.

Further details of these activities can be found in the full version of the Good Practice Guidelines.

PP5 – Implementation

Implementation is the Professional Practice within the BCM Lifecycle that executes the agreed-upon 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 recognize 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-upon 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.

The principles, concepts and assumptions and detailed processes including methods and techniques and outcomes of this professional practice are described in the full version of the Good Practice Guidelines. The following topics are covered:

- The Business Continuity plan – purpose, characteristics and contents
- Developing and managing plans at a strategic, tactical and operational level.

PP6 - Validation

Validation is the Professional Practice within the BCM Lifecycle that confirms that the BCM Program 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.

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.

The principles, concepts and assumptions and detailed processes including methods and techniques and outcomes of this professional practice are described in the full version of the Good Practice Guidelines. The following topics are included:

- Developing an exercise program
- Developing and running an exercise
- Maintaining your BCM program and
- Reviewing your BCM program by using various Auditing methods, including self-assessment.

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.

Thank you for reading the abridged version of The Good Practice Guidelines 2013:

to purchase a full version of this publication please visit the BCI Shop at www.thebci.org

The full version of the GPG is available in the following languages:

- English;
- US English;
- Arabic;
- French;
- German;
- Italian;
- Korean and
- Spanish.

Chinese and Japanese due in 2014.


The Business Continuity Institute
10-11 Southview Park
Marsack Street
Caversham, Reading
Berks RG4 5AF, UK
+44 (0) 118-947 8215

bci@thebci.org
www.thebci.org

Business Continuity Institute